【內部使用】

文件編號：NCCST-C-002

數位國家資通安全技術服務計畫
資通系統風險評鑑參考指引
(V4.1)

行政院資通安全會報技術服務中心
中華民國110年12月修訂

修訂歷史紀錄表

項次	版次	修訂日期	說明
1	V1.0	99/5/28	新編
2	V2.0	100/5/3	1.風險評鑑之高階風險評鑑採用「資通系統分類分級與鑑別機制手冊」方法 2.依機關導入結果修正參考指引
3	V2.0	101/6/19	依機關導入結果修正參考指引
4	V3.0	104/7/24	1.ISO 27005 於民國 100 年修訂 2.ISO 27001 2013 版已將風險評鑑方法指向 ISO 31000，故風險評鑑方法參考 ISO31000 修正
5	V4.0	107/12/20	1.ISO 31000 於民國 107 年改版 2.風險評鑑之高階風險評鑑所採用之「資訊系統分類分級與鑑別機制手冊」已被「資通安全責任等級分級辦法」取代，故修正高階風險評鑑作法 3.修改風險值計算方式在資訊及資通系統資產價值之選取方式 4.依據資通安全維護計畫(範本)修正高階風險評鑑作法與詳細風險評鑑作法之對象
6	v4.1	110/12/31	配合資通安全管理法及其子法施行，並檢視相關國內外之標準，更新本參考指引之內容

報告摘要

報告名稱	資通系統風險評鑑參考指引
資訊等級	☐機密　☐密　☐內部使用　☒普通
相關撰稿人	江衍勳、劉敏慧、李婉萍、林子群
閱讀對象	☒一般主管　☒資安人員　☒資訊人員　☒一般使用者

內容摘要：

「資通系統風險評鑑參考指引修訂報告」(以下簡稱本指引)旨在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，並修正本指引名稱為「資通系統風險評鑑參考指引」。

第 2 章風險管理架構內容，首先說明風險的定義、風險管理之原則、框架與過程之關係，並介紹 ISO 31010 所列舉之風險評鑑技術與方法，最後說明 CNS/ISO/IEC 27005 所描述之「高階風險評鑑」與「詳細風險評鑑」方法等。

第 3 章風險管理過程，以實務範例說明「風險溝通與諮詢階段」、「建立全景階段」、「風險評鑑階段」、「風險處理階段」及「風險監視與審查階段」等 5 大階段管理程序，並以「全球資訊網」舉例說明資通系統風險評鑑之循環程序，提供「資訊人員」、「資安人員」風險管理之實作建議。

關鍵詞	風險、風險管理、風險評鑑、ISO 31000、ISO 31010

目　次

圖 目 次

表 目 次

1. 前言

1.1 目的

資訊系統風險評鑑參考指引前於民國 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，並修正本指引名稱為「資通系統風險評鑑參考指引」(以下簡稱本指引)。

同時因應「資訊系統分類分級與鑑別機制參考手冊」所規範之內容已為資通安全管理法之「資通安全責任等級分級辦法」[1]取代，本指引將協助政府機關資安管理相關人員，了解風險評鑑過程與所採用技術，以評鑑機關資通系統所面臨風險，俾利採取適當的安全防護控制措施，降低資安風險。

政府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，政府機關可參考本指引，針對資通系統與所屬資產進行風險評鑑，但不以此為限，以符合資安相關法規、標準規範之要求。

1.2 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，詳見表 1。

表1　資通系統風險評鑑參考指引適用對象對照表

章	節	款	一般主管	資訊人員	資安人員	一般使用者
2 風險管理架構	2.1 風險的定義	風險的定義	○	○	○	○
	2.2 風險管理之原則、框架與過程	2.2.1 風險管理之原則	○	○	○	△
		2.2.2 風險管理之框架	○	○	○	△
		2.2.3 風險管理之過程	○	○	○	△
	2.3 政府機關風險管理架構	2.3.1 行政院所屬各機關風險管理及危機處理作業基準	○	○	○	△
		2.3.2 風險管理及危機處理作業手冊	○	○	○	△
	2.4 CNS/ISO/IEC 27001 對於風險管理之要求	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	△	○	○	△
	2.5 風險評鑑技術與方法	整理 ISO 31010 所列舉之風險評鑑技術與方法	△	○	○	△
	2.6 CNS/ISO/IEC 27005 資訊系統風險評鑑	2.6.1 高階風險評鑑作法	△	○	○	△
		2.6.2 詳細風險評鑑作法	△	○	○	△
3 風險	3.1 風險溝通與諮詢階段	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	○	○	○	△

章	節	款	一般主管	資訊人員	資安人員	一般使用者
評鑑管理程序	3.2 建立全景階段	3.2.1 風險管理基本準則	○	○	○	△
		3.2.2 資通系統範疇與邊界	○	○	○	△
		3.2.3 風險評鑑組織	○	○	○	△
	3.3 風險評鑑階段	3.3.1 執行「高階風險評鑑作法」	△	○	○	
		3.3.2 執行「詳細風險評鑑作法」	△	○	○	
	3.4 風險處理階段	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	○	○	○	△
	3.5 風險監控與審查階段	3.5.1 風險評鑑報告審查與變更管理	○	○	○	△
		3.5.2 內部稽核	○	○	○	
		3.5.3 外部稽核	○	○	○	
附記	各項符號代表意義說明如下： ○：詳閱 ； △：參考；					

資料來源：本計畫整理

1.3 章節架構

本指引分為前言、風險管理架構、風險管理程序、參考文獻及附件共 5 部分進行撰述，重點摘錄如下：

第 1 章「前言」，說明本指引之目的、適用對象及指引章節架構介紹，協助政府機關於執行資通系統風險評鑑時，對管理目的與本指引架構能有全

盤性的認識。

第 2 章「風險管理架構」，首先說明風險的定義、風險管理之原則、框架與過程之關係，然後介紹政府機關風險管理架構，包含「行政院及所屬各機關風險管理及危機處理作業基準」與「行政院所屬各機關風險管理及危機處理作業手冊」之摘要說明，緊接著描述 CNS/ISO/IEC 27001[2]對於風險管理之要求，並介紹 ISO 31010[3]所列舉之風險評鑑技術與方法，最後說明 CNS/ISO/IEC 27005[4]描述之「高階風險評鑑」與「詳細風險評鑑」方法等，以及本指引之建議作法。

第 3 章「風險管理程序」，包含「風險溝通與諮詢階段」、「建立全景階段」、「風險評鑑階段」、「風險處理階段」及「風險監視與審查階段」等 5 大階段管理程序，並以「全球資訊網」舉例說明資通系統風險評鑑之循環程序。

「3.1 風險溝通與諮詢階段」，應在風險管理初期階段，發展溝通與諮詢方法，俾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，於管理風險上所達成協議的活動，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，政府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。

「3.2 建立全景階段」，政府機關應先行識別機關內、外各方面的安全需求與界定風險評鑑範圍，並清查盤點該範圍內所有相關資通系統，同時規劃與定義該機關之「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，最後整合這些資通系統與資訊及資通系統資產可能涉及的跨部門業務成員，共同組成資通系統風險評鑑組織，將有助於執行與落實風險評鑑的成效。

「3.3 風險評鑑階段」，根據本指引第 2 章所提出的資通系統風險風險管理之過程，以「資通系統」，為輸入對象，並以「循環式」(又稱：迭代式)方式實施資通系統之風險評鑑，分別針對高階風險評鑑作法、詳細風險評鑑作法等 2 種風險評鑑作法之可能風險評鑑循環程序進行說明，政府機關可依據實際狀況，在考量可運用資源下，彈性選擇不同風險循環的組合。

「3.4 風險處理階段」，描述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。

「3.5 風險監視與審查階段」，說明政府機關必須因應法律規章與合約、資安政策異動、內外環境變化、資訊及資通系統資產調整、資安檢查結果及資安事件應變進行風險評鑑報告之審查與變更，同時說明「內部稽核」與「外部稽核」的作法，以確保風險評鑑與安控措施實施之有效性。

第 4 章「參考文獻」，詳列本指引所參考的文件或資料。

第 5 章「附件」，詳列本指引所納編之附件內容。

另為協助政府機關人員快速了解本指引精髓，特編訂「資通系統風險評鑑參考指引導引手冊」，詳見附件 8。

1.4 本次修訂重點

本次修訂重點主要因應 ISO 31000 已於 2018 年 2 月 15 日改版，對於風險之原則、框架及過程已進行部分修正。ISO 31000：2018 提供比 ISO 31000：2009 更具策略性的指導意見，並更加重視高階管理層的參與及將風險管理整合到組織中，包括建議制訂一份聲明或政策，以確認對風險管

理的承諾，並確保投入必要的資源進行風險管理，還建議將風險管理做為組織架構、流程、目標、策略及活動的一部分。

原高階風險評鑑所採用之「資訊系統分類分級與鑑別機制手冊」之內容，已由「資通安全責任等級分級辦法」取代，故修正高階風險評鑑作法相關內容。

風險值計算方式之資訊及資通系統資產價值原以機密性、完整性、可用性鑑價採相加法，本次修訂資訊及資通系統資產價值改以機密性、完整性、可用性鑑價採取最高值法。

1.5 使用建議

ISO/IEC 27001 已於 2013 年 10 月 1 日改版，CNS 27001 標準隨後於 2014 年 4 月 24 日修訂，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。

第二章風險管理架構內容，有助於「一般主管」、「資訊人員」、「資安人員」及「一般使用者」釐清風險管理之過程，識別政府機關參與者之角色與責任及可採行之標準與評鑑技術。

說明 ISO 31000:2018 強調政府機關所有活動均涵蓋在風險管理範圍內，需對風險進行識別與分析，並評估風險處理方法的影響，符合政府機關之風險條件，以達成機關之目標，明確陳述風險管理之原則、架構與過程之關係。ISO 31010:2009 提供系統化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，亦包含資安所適用之風險評鑑方法。

「行政院及所屬各機關風險管理及危機處理作業原則」[5]及 CNS/ISO/IEC 27005 資訊安全風險管理之過程，均符合 ISO 31000 之風險管理過程要求，所採用之風險評鑑技術與方法，資通安全管理法之「資通安全責任等級分級辦法」建議之方法，亦參考 ISO 31010 所列舉適用於資安管理之風

險評鑑技術與方法之一。

第三章風險管理過程，以實務範例說明「風險溝通與諮詢階段」、「建立全景階段」、「風險評鑑階段」、「風險處理階段」及「風險監視與審查階段」等 5 大階段管理程序，並以「全球資訊網」舉例說明資通系統風險評鑑之循環程序，提供「資訊人員」、「資安人員」風險管理之實作建議。

2. 風險管理架構

2.1 風險的定義

參考 ISO 31000:2018，風險的定義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，所稱組織係指適用於各種類型與大小之公務與非公務機關。

組織目標可包含不同面向，如財務、健康、安全及環保等目標，可應用於不同階層，上至組織策略、專案工作，下至產品發展與過程或資安等，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，包含事件發生的改變程度與發生的可能性等。

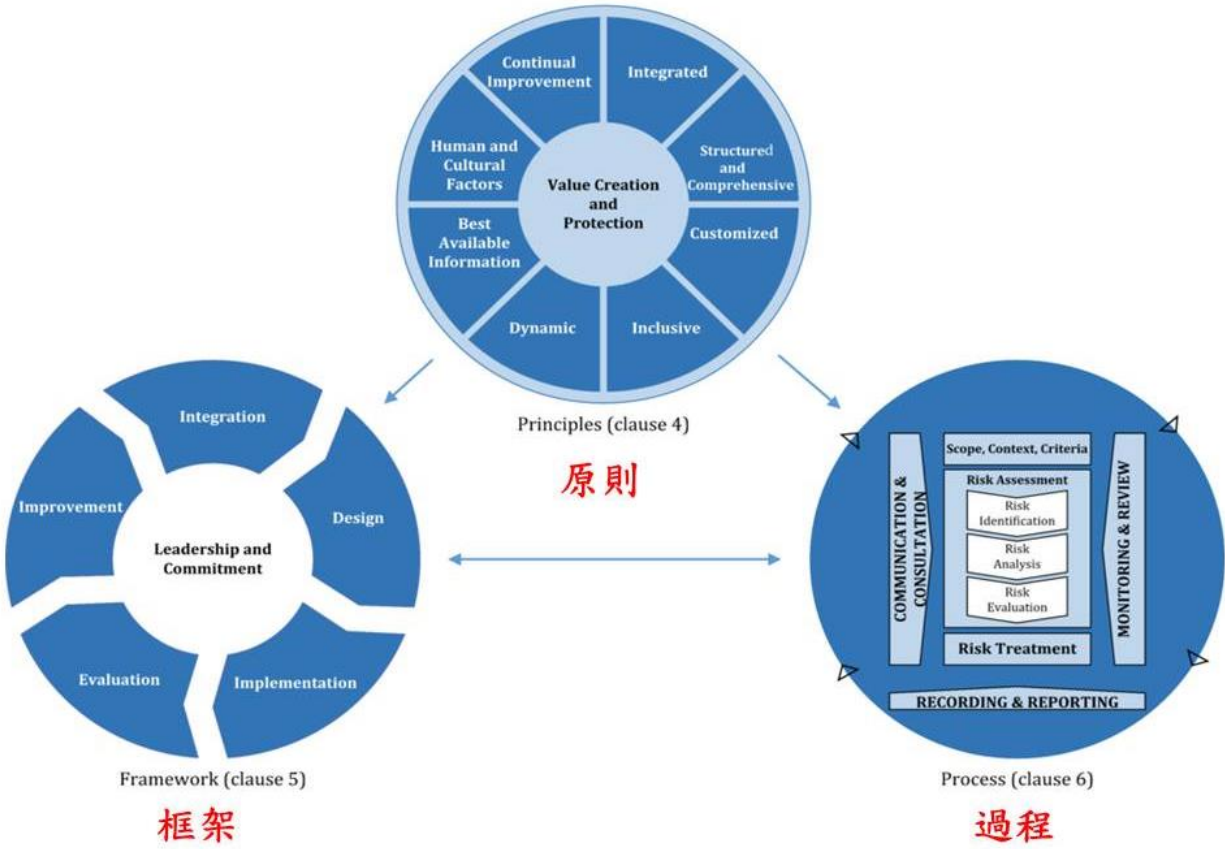
換言之，風險意指任何類型與大小的組織，為達成組織的目標，所面對內部及外部因素影響的不確定性，包含事件發生的改變程度與發生的可能性等。

2.2 風險管理之原則、框架與過程之關係

風險管理係指協同所有之活動加以指導，並控制組織所關注之風險。

政府機關所有活動均涵蓋於風險管理範圍內，需對風險進行識別與分析，並評估風險處理方法的影響，符合機關之風險條件，以達成機關之目標。

以下參考 ISO 31000:2018，說明有關風險管理之原則、框架及過程，詳見圖 1。



資料來源：本計畫整理

圖1　風險管理之原則、框架與過程之關係

2.2.1 風險管理之原則

ISO 31000 指出風險管理的目的是創造與保護資產的價值，規範的原則為風險管理提供有效果且有效率的指導，傳達其價值並解釋其意圖與目的。ISO 31000 提供風險管理原則的聲明，詳見圖 1，說明如下：

- 原則 1：框架與過程應該客製化且互相對應。
- 原則 2：利害關係人必須適當與及時的參與。
- 原則 3：採用結構與全面的方法。
- 原則 4：風險管理是組織所有活動的一部分。

●原則 5：風險管理應依預測、發現、告知及反應而執行變更。

●原則 6：風險管理應考慮可用資訊的限制。

●原則 7：風險管理的各個面向都會受到人文因素影響。

●原則 8：風險管理透過學習與經驗不斷改進。

前 5 項原則為設計風險管理措施提供指導，原則 6、7 及 8 則是與風險管理運作有關措施。

前 5 項原則涉及風險管理措施的設計與規劃，且這些原則經常被歸納為比例性(proportionate)、一致性(aligned)、全面性(comprehensive)、嵌入性(embedded)及動態性(dynamic)，簡稱 PACED，詳見表 2。

表2　風險管理原則前 5 項歸納

原則	描述
比例性	風險管理活動必須與組織所面臨的風險成比例
一致性	風險管理活動需要與組織內其他活動保持一致
全面性	為了充分發揮作用，風險管理方法必須是全面
嵌入性	風險管理活動需要嵌入到組織中
動態性	風險管理活動必須是動態的，並對新興和有影響的事物作出改變

資料來源：https://www.theirm.org/media/3513119/IRM-Report-ISO-31000-2018-v3.pdf

2.2.2 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與組織的所有其他活動中，如組織在進行決策

時，即應將風險管理納入考量，詳見圖 2。

●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、計畫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

– 制定適當的實施計畫，包括最後期限等。

– 定義由誰於何時、何處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。

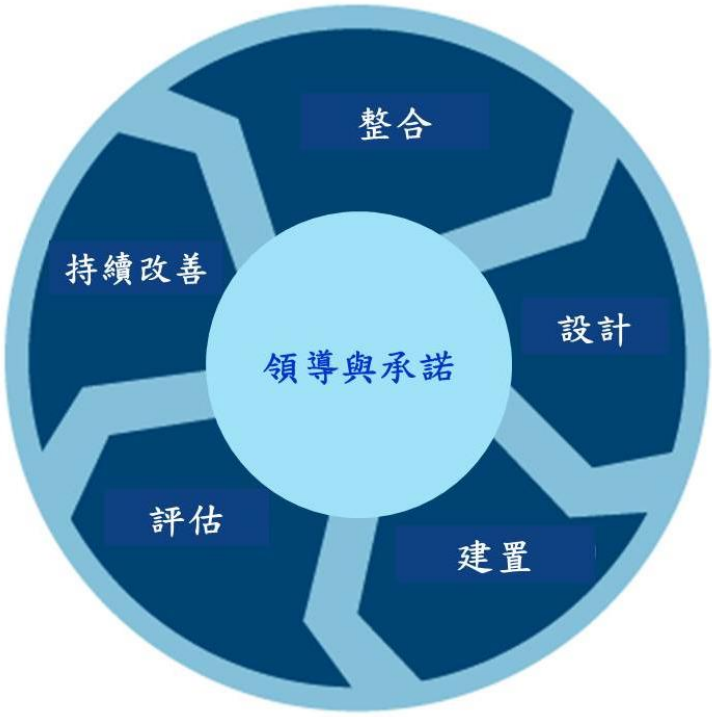
– 確定風險管理框架是否仍適用於實現組織目標。

●持續改善

– 不斷監測與調整框架以解決外部與內部變化。

– 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：本計畫整理

圖2　風險管理之框架

2.2.3 風險管理之過程

風險管理過程以系統化將政策、程序及實踐，應用於溝通及諮詢、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，詳見圖 3。

資料來源：本計畫整理

圖3　風險管理之過程

●溝通及諮詢

– 於風險管理過程之各階段協同不同領域專家。

– 協助從不同的觀點定義風險條件與評估。

– 提供足夠的資訊來促進風險監督與決策。

– 對受風險影響的人建立具包容性(inclusiveness)與歸屬感(ownership)的意識。

●範圍、全景及準則

– 界定風險管理活動的目的與範圍。

– 界定組織的外部與內部環境。

– 界定可接受風險與類型的風險準則。

– 界定評估風險重要性與支持決策的準則。

●風險評鑑

– 風險鑑別主要在發現、識別及描述可能有助於或阻止目標實現及各種有形或無形的風險影響。

– 對風險的類型與特徵進行風險分析，包括風險等級、風險來源、後果、可能性、事件、情境、控制及其有效性。

– 風險評估係透過比較風險分析結果與使用的風險準則，確定風險的重大性以支持決策。

●風險處理

– 選擇最合適的風險處理方案。

– 設計風險處理計畫，明訂如何實施處理選項。

●監視與審查

– 提高過程設計、實施及結果的質量與有效性。

– 監視風險管理流程及其結果，監視與審查的責任須清楚界定。

– 計畫、收集及分析所得資訊、記錄其結果，並提供回饋。

– 將結果納入績效管理、衡量及報告活動。

●記錄與報告

– 在整個組織內溝通風險管理活動與結果。

– 為決策提供資訊。

– 改進風險管理活動。

– 提供風險資訊並與利害相關者進行互動。

2.3 政府機關風險管理架構

鑒於自然、人文社會環境快速變遷，政府機關施政面臨之風險日益增加，主要先進國家已將風險管理納入政府改革重點，行政院為改善所屬各部、會、行、處、局、署、院(以下簡稱各部會)機關治理、降低財務損失、提升運作效益、達成施政目標，及掌握創新突破機會，以防範及消減施政風險之衝擊，並促使各部會將風險管理融入日常作業及決策運作。為引導各機關進行風險管理工具之實務性操作，依據行政院於 109 年 9 月 11 日函頒「行政院及所屬各機關風險管理及危機處理作業原則」第 4 點之授權規定，國家發展委員會會同行政院主計總處研訂「行政院及所屬各機關風險管理及危機處理作業手冊」[6]，於 109 年 9 月 28 日函頒，並配合作業原則之施行日，亦自 110 年 1 月 1 日生效，協助各部會了解風險管理與危機處理之實務運作。

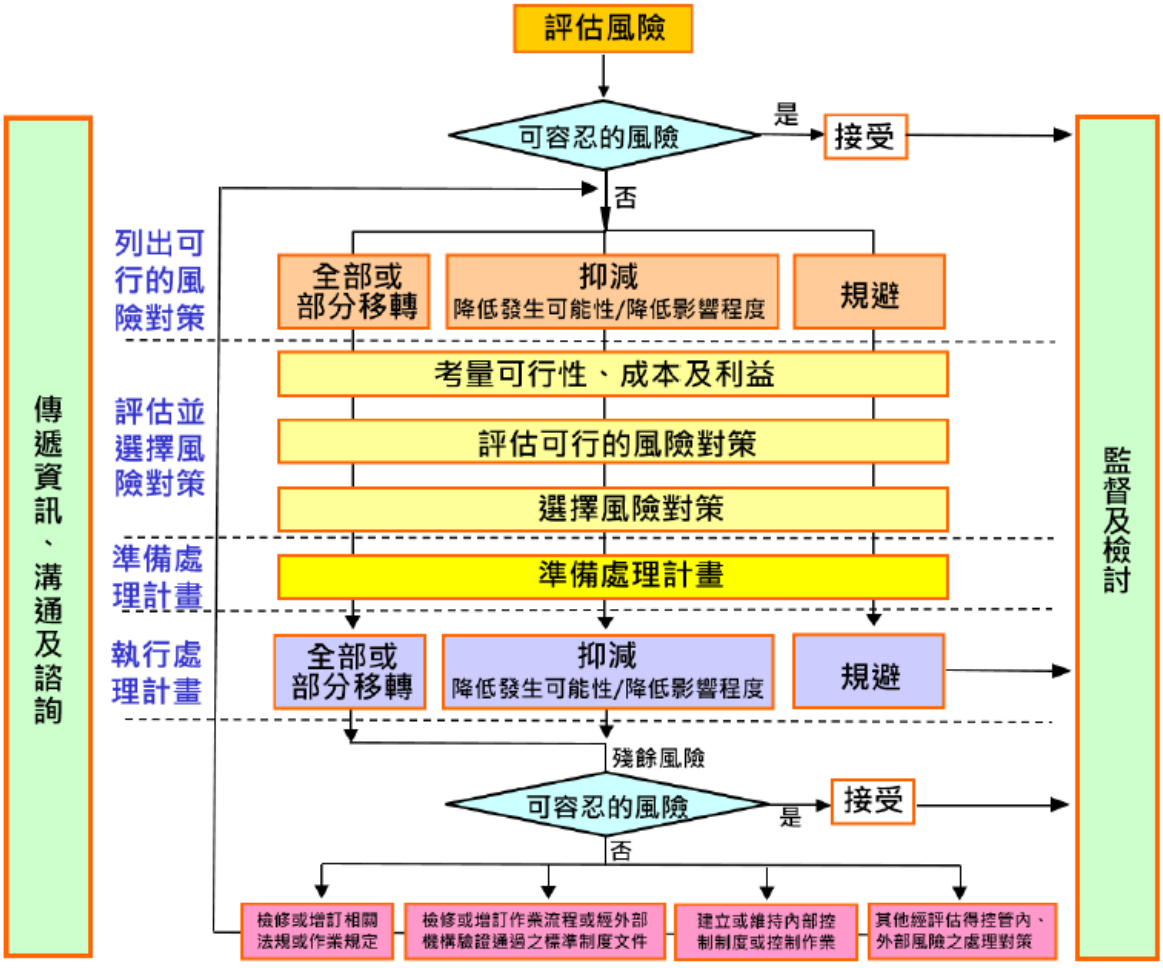
2.3.1 行政院及所屬各機關風險管理及危機處理作業原則

行政院訂定本作業原則之目的為推動行政院及所屬各機關、公立學校將風險管理融入日常作業及決策運作，考量可能影響施政目標達成之風險，訂定機關之施政目標及策略，並透過辨識及評估風險，採取內部控制或其他處理機制，以合理確保達成施政目標；並於危機事件發生時，採取危機處理，降低對機關損害之影響程度。

本作業原則所稱風險管理，指為有效管理可能發生事件並降低其不利影響所執行之步驟及過程；其包含內部控制之建立及執行，透過控制環境、風險評估、控制作業、資訊與溝通及監督作業，事先整合機關內部各種控管及評核措施，降低各機關施政目標無法達成之內部風險。

2.3.2 行政院及所屬各機關風險管理及危機處理作業手冊

「行政院及所屬各機關風險管理及危機處理作業手冊」強調風險管理是一個「持續改善」的反覆過程或循環過程，並建議參考之風險管理架構，詳見圖 4，以協助政府機關改善績效並達成公共價值(Public Value)，另可促成行政部門提供更好的服務、資源的更有效使用、更佳的計畫管理、避免貪瀆與浪費公帑並鼓勵創新。相反的，若缺乏風險管理，人民與企業可能因公共服務不當與沒有效率的服務而浪費時間與金錢，政府機關的聲望可能因服務無法符合社會大眾的期望而受損。因此，風險管理的核心價值不僅在於降低威脅，更是追求政府機關的創新機會與公眾價值。



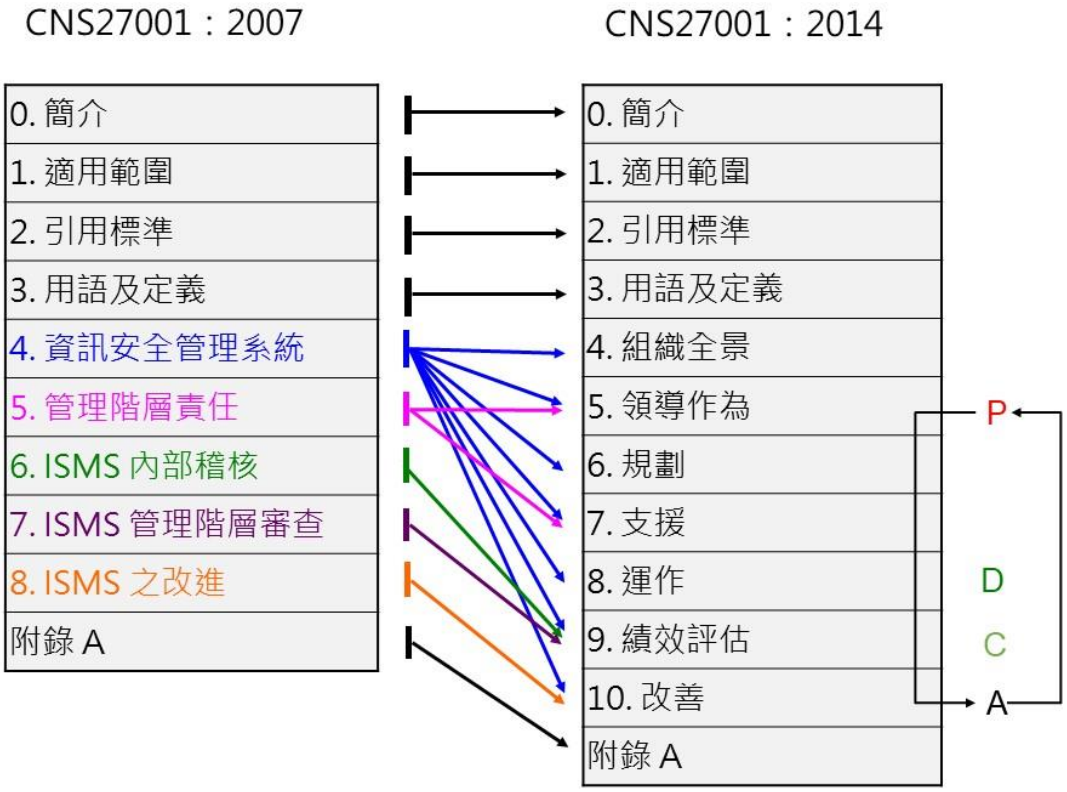
資料來源：行政院及所屬各機關風險管理及危機處理作業手冊

圖4　行政院建議之風險管理架構

行政院建議之風險管理架構，係參考 ISO 31000 之風險管理過程所訂定，並依據行政院及所屬各機關之實務需求加以調整，做為各級政府機關之指導與建議。

2.4 CNS/ISO/IEC 27001 對於風險管理之要求

ISO/IEC 27001 目前版本為 2013 年 10 月 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 5。



資料來源：本計畫整理

圖5　CNS 27001 內容架構

CNS/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)。

2.5 風險評鑑技術與方法

CNS 31010[7] 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，亦包含資安所適用之風險評鑑方法，詳見表 3。

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3　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	

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		
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	
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	

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		
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	
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 建議之資安風險評鑑風法： 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					

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		

資料來源：CNS 31010 附錄 A

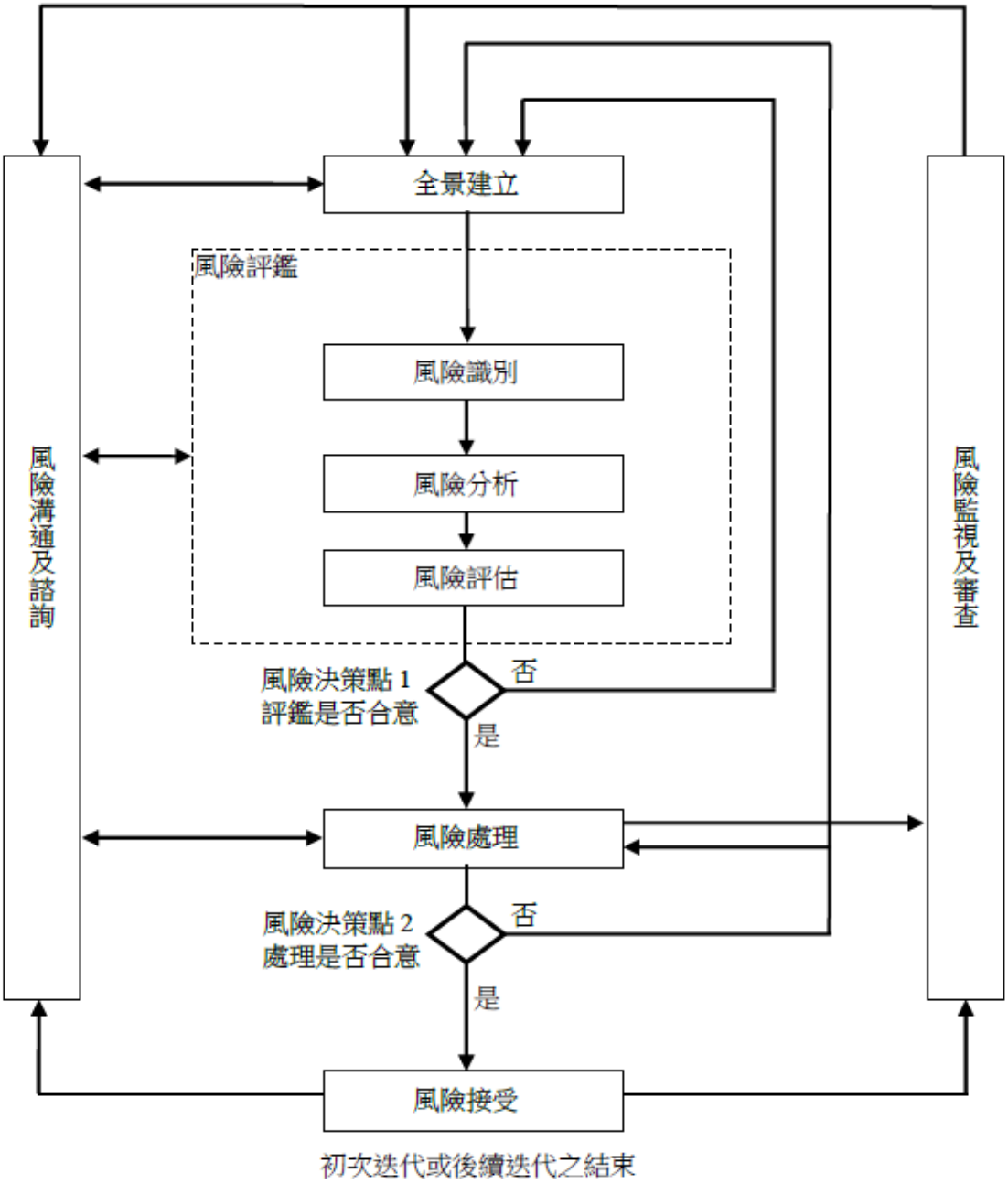
2.6 CNS/ISO/IEC 27005 資訊系統風險評鑑

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，相關修訂內容詳見標準之附錄 G。

本標準提供組織之資安風險管理指導綱要，並支援 CNS/ISO/IEC 27001:2013 資訊安全管理系統(Information Security Management System, ISMS)之特定要求。

本標準並不提供任何資安風險管理之特定方法論，組織可自行依據資安管理系統(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。目前常用之方法論，已可在本標準之框架下，實作資安管理系統(ISMS)之要求。

風險管理過程的高階觀點係遵循 ISO 31000 之規定，資安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，在每一循環中增加評鑑之深度與詳細度。循環作法提供以最小化花費，在識別控制措施之時間與耗費間取得良好平衡，以確保高風險被適當評鑑，詳見圖 6。



資料來源：CNS 27005

圖6　資安風險管理過程

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修正風險至可接受等級所需之措施，則評鑑工作完成後即展開風險處理。若資訊不充分，則需再進行一次修訂全景(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，詳見圖 6 風險決策點 1。

風險處理之有效性係依風險評鑑結果而定，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(如風險評鑑、風險接受或衝擊準則)，進行另一次風險評鑑循環，再執行更進一步之風險處理，詳見圖 6 風險決策點 2。

換言之，CNS/ISO/IEC 27005 所描述之資安風險管理過程，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」所陳述之管理架構一致，均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 種資安風險評鑑作法，說明如下。

2.6.1 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，詳見表 4。

表4　資通系統企業衝擊分析範例

安全等級 / 影響構面	普	中		高	
	0	1	2	3	4
1. 機密性	未經授權之資訊揭露，在機關營運、資產或信譽等方面，造成可預期之	未經授權的資訊揭露，在機關營運、資產或信譽等方面，造成可預期之		未經授權之資訊揭露，在機關營運、資產或信譽等方面，造成可預期之	

安全等級 影響構面	普	中		高	
	0	1	2	3	4
	有限負面影響，如： ▪ 一般性資料；資料外洩不致影響機關權益或僅導致機關權益輕微受損。	嚴重負面影響，如： ▪ 敏感性資料；資料外洩將導致機關權益嚴重受損 - 涉及區域性或地區性個人資料，包含出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、聯絡方式、財務情形、社會活動及其他得以直接或間接識別個人之資料。		非常嚴重或災難性負面影響，如： ▪ 機密性資料；資料外洩將危及國家安全、導致機關權益非常嚴重受損 - 凡涉及國家安全之外交、情報、國境安全、財稅、經濟、金融、醫療等重要機敏系統。 - 特殊屬性之個人資料（如臥底警員、受保護證人、被害人等資料等），資料外洩可能會使相關個人身心受到危害、社會地位受到損害、或衍生財物損失等情形。	

安全等級 影響構面	普	中		高	
	0	1	2	3	4
				- 涉及個人之醫療、基因、性生活、健康檢查、犯罪前科等資料，資料外洩將使個人權益非常嚴重受損，如醫療資訊系統、刑案資訊整合系統等。 - 涉及全國性個人資料，包含出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、聯絡方式、財務情形、社會活動及其他得以直接或間接識別個人之資料，如	

安全等級 影響構面	普	中		高	
	0	1	2	3	4
				戶役政資訊系統、護照管理系統等。	
2. 完整性	未經授權之資訊修改或破壞，在機關營運、資產或信譽等方面，造成可預期之有限負面影響，如： ▪ 資料遭竄改不致影響機關權益或僅導致機關權益輕微受損。	未經授權之資訊修改或破壞，在機關營運、資產或信譽等方面，造成可預期之嚴重負面影響，如： ▪ 資料遭竄改將導致機關權益嚴重受損。		未經授權之資訊修改或破壞，在機關、資產或信譽等方面，造成可預期之非常嚴重或災難性負面影響，如： ▪ 資料遭竄改將危及國家安全、導致機關權益非常嚴重受損。	
3. 可用性	資訊、資通系統之存取或使用上的中斷，在機關營運、資產或信譽等方面，造成可預期之有限負面影響，如： ▪ 系統容許中斷時間較長（如 72 小時）。 ▪ 系統故障對社會秩序、民生體系運作不致造成影響或僅有輕微影響。	資訊、資通系統之存取或使用上的中斷，在機關營運、資產或信譽等方面，造成可預期之嚴重負面影響，如： ▪ 系統容許中斷時間短。 ▪ 系統故障對社會秩序、民生體系運作將造成嚴重影響。		資訊、資通系統之存取或使用上的中斷，在機關營運、資產或信譽等方面，造成可預期之非常嚴重或災難性負面影響，如： ▪ 系統容許中斷時間非常短（如 30 分鐘）。 ▪ 系統故障對社會秩序、民生體系運作將造成非常嚴重影響，甚至危及國家安全。	

安全等級 影響構面	普	中		高	
	0	1	2	3	4
	▪ 系統故障造成機關業務執行效能輕微降低。	▪ 系統故障造成機關業務執行效能嚴重降低。		▪ 系統故障造成機關業務執行效能非常嚴重降低，甚至業務停頓。	
4. 影響法律規章遵循	系統運作、資料保護、資訊及資通系統資產使用等若未依循相關法律規範辦理，造成可預期之有限負面影響，如： ▪ 全球資訊網：必須符合智慧財產權相關法令尊重他人智慧財產，並遵守兒童及少年福利與權益保障法進行資訊內容管理，否則將涉及違反法律之遵循性。	系統運作、資料保護、資訊及資通系統資產使用等若未依循相關法律規範辦理，造成可預期之嚴重負面影響，如： ▪ 政府電子採購網：依「政府採購法」第 27 條規定，機關辦理公開招標或選擇性招標，應將招標公告或辦理資格審查之公告刊登於政府採購公報或公開於資訊網路。因此，若系統資料遭竄改導致公告資料錯誤，將影響採購作業透明化。		系統運作、資料保護、資訊及資通系統資產使用等若未依循相關法律規範辦理，造成可預期之非常嚴重或災難性負面影響，如： ▪ 機密性資料：依「國家機密保護法施行細則」第 28 條第 4 款規定，國家機密之保管方式直接儲存於資訊系統者，須將資料以政府權責主管機關認可之加密技術處理，該資訊系統並不得與外界連線。因此，機關若未依循規定儲存資料，將涉及從根本上違反法律之遵循性。	

安全等級 影響構面	普	中		高	
	0	1	2	3	4
				▪ 醫療機構醫囑暨電子病歷系統：依「醫療機構電子病歷製作及管理辦法」第 3 條、第 4 條規定，電子病歷資訊系統之建置、電子病歷之製作及儲存應符合相關規定。因此，機關若未依循相關規定進行系統建置維運及資料儲存，將涉及從根本上違反法律之遵循性。	

資料來源：本計畫整理

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，以建構機關資安之策略藍圖。

●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。

2.6.2 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 附錄 E，列舉符合 ISO 31010 之後果/機率矩陣(Consequence/probability matrix)，本指引參考該矩陣提供 2 個實務範例，但不以此為限，說明如下。

預先定義值矩陣主要考量資產之價值、威脅發生之可能性及脆弱性被利用之程度，以排序待因應之風險，其範例(一)詳見圖 7，說明如下。

	發生可能性－威脅	低			中			高		
	易被利用	低	中	高	低	中	高	低	中	高
資產價值	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

資料來源：CNS 27005

圖7　預先定義值矩陣範例(一)

●資產價值

依據資產之建置成本或置換成本加以估價，再轉換成對應的量測尺度。

資產之價值可經由與資料擁有者之訪談，依據不利之營運後果可合理預

期發生之最壞情境加以估計。經訪談後設定置換成本，再轉換成量測尺度，細分為 0~4 之 5 等級區分，以表示資產之價值，另實務中對於資訊及資通系統資產之衡量，亦會採用評估「機密性 C」、「完整性 I」與「可用性 A」之組合[CIA]加以衡量。

資產價值之[CIA]組合表示，分成以下 2 種模式：

資產價值[CIA]＝C + I + A 或

資產價值[CIA]＝C x I x A

(若採用相乘之方式，建議將上述之量測尺度修訂為 1~5 等級區分，以避免相乘之後，產生資產價值為 0 之情形。)

不論採用相加或相乘之計算模式，經轉換成量測尺度之後，所代表之意義均是排序後之結果，代表待因應風險的優先順序，至於要採用相加或相乘方法，可視機關之需求與量測尺度範圍而定，並無優劣之分。

●發生可能性—威脅

將威脅發生之可能性，區分為低、中、高 3 級。

●脆弱性易被利用之程度

再將威脅利用脆弱性之容易程度，區分為低、中、高 3 級。

經由以上方法識別風險之相關量測組合，尺度由 0~8，填入於矩陣之內。

另一範例(二)顯示類似之矩陣，分析營運衝擊之程度，另考量事件情境發生之可能性，以排序風險處理之優先順序。

縱軸將營運衝擊程度由非常低至非常高，區分為 5 個尺度，分別為 0~4。

橫軸將事件情境之可能性由非常低至非常高，區分為 5 個尺度，分別為 0~4。再將兩軸之尺度值相加，產生 0~8 尺度，詳見圖 8。

以上範例所列示之 0~8 尺度，可再簡化成為整體風險等級，例如：

●低風險：0~2。

●中風險：3~5。

●高風險：6~8。

	事故情境之可能性	非常低 (非常不可能)	低 (不可能)	中 (有可能)	高 (可能)	非常高 (經常)
營運衝擊	非常低	0	1	2	3	4
	低	1	2	3	4	5
	中	2	3	4	5	6
	高	3	4	5	6	7
	非常高	4	5	6	7	8

資料來源：CNS 27005

圖8　預先定義值矩陣範例(二)

2.6.2.1 依風險之量測排序威脅

本方法將後果(資產價值)之因素與威脅發生之可能性(將脆弱性層面納入考量)相互關聯，詳見圖 9。

威脅描述詞 (a)	後果(資產) 值 (b)	威脅發生 可能性 (c)	風險量測 (d)	威脅排序 (e)
威脅 A	5	2	10	2
威脅 B	2	4	8	3
威脅 C	3	5	15	1
威脅 D	1	3	3	5
威脅 E	4	1	4	4
威脅 F	2	4	8	3

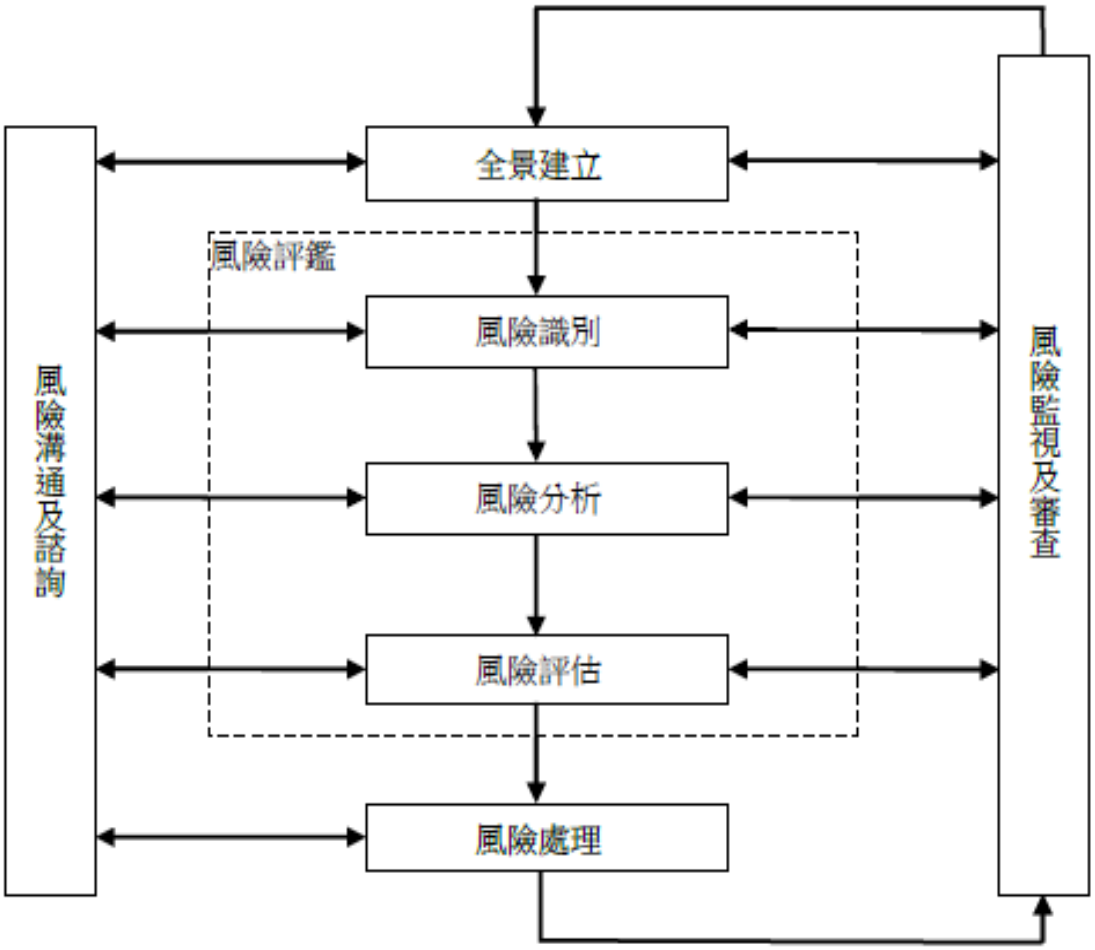
資料來源：CNS 27005

圖9　依風險之量測排序威脅之範例

- 首先依據預先定義之尺度，範例中採用的是 1~5，評估各受威脅資產之後果(資產價值) (b 欄位)。
- 同樣依預先定義之尺度 1~5，評估各威脅發生之可能性(c 欄位)。
- 藉由相乘(b x c)計算風險之量測。
- 最後再依風險相關之量測順序排序威脅(e 欄位)。

3. 資通系統風險管理過程

本指引主要在協助政府機關資安管理人員了解風險評鑑技術，以評鑑機關資通系統風險，俾利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 10。



資料來源：本計畫整理

圖10 資通系統風險管理過程

3.1 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，俾利風險管理過程中各階段，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，於風險管理上達成協議的活動，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、處理之方法及風險可接受之程度等。

機關應納編各部門成員及各領域專家，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被了解並納入考量。

●協助確認風險已被充分的識別。

●協同不同領域專家進行風險分析。

●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。

為讓負責實施風險管理的人員了解決策的基礎，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，因此，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發言人合作，以協調風險溝通相關事務。

執行風險溝通與諮詢，期達到以下目的：

●提供組織風險管理結果並提供保證。

●蒐集風險資訊。

●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了解，而導致資安漏洞之發生與後果。

●支援決策者所作決策。

●取得新的資安知識。

●與其他機關協調並規劃應變機制，以降低任何事件所造成之後果。

●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。

3.2 建立全景階段

政府機關應依資通安全管理法及其施行細則要求，訂定資通安全維護計畫，每年度應盤點資訊及資通系統資產，並製作「資訊及資通系統資產清冊」，據以執行風險評鑑，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。

另外，實作風險評鑑之前，政府機關也應先將風險評鑑範圍界定出來，並清查盤點該範圍內所有相關資通系統，同時整合這些資通系統與資訊及資通系統資產可能涉及的跨部門業務成員，共同組成資通系統風險評鑑組織，將有助於執行與落實風險評鑑的成效。

3.2.1 基本準則

參考本指引或 CNS/ISO/IEC 27005:2011，落實風險評鑑的執行，政府機關應發展適用於該機關之風險管理基本準則，其中包含「風險管理作法」、「風險評估準則」、「衝擊準則」及「風險接受準則」，說明如下。

3.2.1.1 風險管理作法

政府機關應依據資通安全管理法及其施行細則，參考資通安全維護計畫(範本) ，每年針對資訊及資通系統資產進行「詳細風險評鑑方法」進行風險評估，另自行或委外開發之資通系統應每年依據資通安全責任等級分級辦法之規定，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，並參考「安全控制措施選擇參考指引」，選擇適當之安全控制措施，進行風險處理作業。

3.2.1.2 風險評估準則(Risk Evaluation Criteria)

風險評估準則的主要目的在於決定風險處理之優先順序，政府機關應發展風險評估準則，並納入以下之考量因素，以評估資安風險：

- 執行風險評鑑及建立風險處理計畫。
- 定義及實作政策及程序，內容應包含所有控制措施之實作。
- 監視控制措施。
- 監視資安風險管理過程。

採用詳細風險評鑑作法者，風險評估準則應包含：

- 後果評鑑(亦可視為：資訊及資通系統資產價值)之準則。

  資訊及資通系統資產價值評定方式有相加、相乘、取最大值等方式，但經轉換成量測尺度，所代表的是資訊及資通系統資產價值的優先順序，

對於整體風險管理而言並無差異。

有關鑑別資訊及資通系統資產價值，可在資訊及資通系統資產發生事件時，以破壞「機密性」、「完整性」及「可用性」造成的後果，鑑別資訊及資通系統資產的價值，說明如下：

– 機密性

- 普，其價值為 1：漏失資訊之機密性保護，所造成後果輕微或可忽視者。
- 中，其價值為 2：漏失資訊之機密性保護，所造成的後果嚴重且其災害會影響業務。
- 高，其價值為 3：漏失資訊之機密性保護，所造成的後果很嚴重且其災害會影響業務深遠或信譽受損。

– 完整性

- 普，其價值為 1：若缺乏完整性保護，所造成後果是輕微或可忽視者。
- 中，其價值為 2：若缺乏完整性保護，會造成組織嚴重的後果，且其災害會影響組織業務運作。
- 高，其價值為 3：若缺乏完整性保護，會造成組織很嚴重的後果，且其災害會影響組織業務停頓或信譽受損。

– 可用性

- 普，其價值為 1：若缺乏可用性保護，所造成後果是輕微或可忽視者。
- 中，其價值為 2：若缺乏可用性保護，所造成的後果嚴重，且其災害

會影響業務。

- 高，其價值為 3：若缺乏可用性保護，所造成的後果很嚴重，且其災害會嚴重影響業務者或信譽受損。

●威脅發生之可能性準則

– 普，其值為 1：發生可能性低，沒發生過或不可能發生。

– 中，其值為 2：發生可能性中等，曾發生過但次數很少。

– 高，其值為 3：發生可能性高，過去經常發生。

●脆弱性被利用之容易程度準則

– 普，其值為 1：很難被利用。

– 中，其值為 2：被利用的難易度適中。

– 高，其值為 3：很容易被利用。

以政府機關所擁有之個資為例，在機密性部分，若資料經處理後無法達到足資識別當事人者，視為「普」級；若資料經組合可達到直接或間接識別當事人者，則視為「中」級；若資料包含當事人之病歷、醫療、健康檢查、基因、性生活及犯罪前科等資料者，則視為「高」級。

有關以上所述之評估準則，詳細內容詳見 3.3 風險評鑑階段之範例說明。

3.2.1.3 衝擊準則(Impact Criteria)

衝擊準則主要在訂定當威脅與脆弱性結合時，資訊及資通系統資產的「機密性」、「完整性」及「可用性」遭破壞，對於組織衝擊的嚴重性，可能包括營運的受損、信譽的損害、資安的危害、業務與財務價值的損失及違

法情事等，建議將衝擊的嚴重性以「機密性」、「完整性」及「可用性」遭破壞的程度分為 3 等級（普、中、高），分別說明各等級對組織的影響。

如「機密性」之「普」級為公開資訊缺乏機密性保護，所造成後果輕微或可忽視者。「完整性」之「中」級為缺乏完整性保護，造成組織嚴重的後果，且其災害會影響組織業務運作。「可用性」之「高」級為缺乏可用性保護，造成的後果很嚴重，且其災害會嚴重影響業務或信譽受損。

3.2.1.4 風險接受準則(Risk Acceptance Criteria)

風險接受準則的主要目的在於決定風險處理範圍，政府機關會因其所負責任務的類別與性質、服務對象、內部資源及經費預算等因素，影響其風險處理範圍。在有限資源內，決定那些風險因影響層面較大需優先進行處理，那些風險因影響層面較小，在資源不足情況下暫時予以接受而保留該等風險。以某中央部會為例，其機密資料的保護是最重要的，不允許任何機密資料外洩而造成機關信譽受損，故在「機密性」上的要求高於「可用性」與「完整性」。因此，該機關會將可能外洩機密資訊的風險列為最優先處理部分，以確保機密資訊受到適當的保護。「機密資料外洩而造成機關信譽受損」是該機關「不可承受的風險」，故其風險接受準則可為「管控機密資料外洩的風險，以維護本機關信譽」。以提供「便民服務」為主的某機關為例，其業務服務的正確性與持續性最重要，不允許任何「便民服務」停頓或中斷超過 4 小時，因此在「完整性」與「可用性」上的要求高於「機密性」，且「便民服務」的業務持續運作措施須於 4 小時內完成。因此，該機關將可能破壞「完整性」與「可用性」的風險列為最優先處理部分，以確保服務之正確性與持續性。「服務不正確、中斷與停頓」是該機關「不可承受的風險」，故其風險接受準則可為「管控服務的正確性與持續性，以維護本機關信譽」。由前述例子可知，風險接受準則因機

關負責任務不同，而考量的重點也不同，可能影響風險接受準則項目說明如下：

●業務需求與目標。

●法律、法令、規章及合約方面的要求

各機關所適用的法律、法令與規章或許有些差異，本指引列出一些對政府機關絕對必要的共通部分以供參考：

– 資通安全管理法及其施行細則與相關子法。

– 國家機密保護法。

– 人格權與隱私(如個人資料保護法等)。

– 組織檔案紀錄的保護。

●智慧財產權(Intellectual Property Right, IPR)。

●資源分配狀況。

●技術成熟度。

●經費預算。

●社會與人道主義因素。

3.2.2 資通系統範疇與邊界

政府機關在進行資通系統風險評鑑之前，可清查所有資通系統與施政業務的關聯，以做為資安風險管理之範疇與邊界。

在定義風險管理之範疇與邊界時，應考量以下項目：

●機關之營運目標、策略及政策。

●施政業務之維運過程。

●機關之功能及結構。

●適用之法令、法規及契約之要求。

●機關之資安政策。

●整體風險管理作法。

●機關之資訊及資通系統資產。

●機關所在之位置與地理條件。

●影響機關之限制條件。

●利害關係人之期望。

●社會文化環境。

對於排除資安風險管理範疇外之事項，應敘明理由。

3.2.3 風險評鑑組織

本指引建議政府機關應成立「跨部門」之風險評鑑組織，一般通常認為資訊人員與資安人員最清楚資訊技術，所以應由資訊人員或資安人員來執行風險評鑑，惟應考量各業務單位相關資訊及資通系統資產的風險與資產的重要性，最熟悉者為各單位實際執行業務的承辦人員，因此「風險評鑑組織」成員宜包含施政業務與支援該業務之資通系統相關人員，如資訊、資安、總務、人事及業務人員，避免由單一成員執行所有資通系統風險評鑑工作，因而導致產出結果過於主觀，不符合真實情況。

風險評鑑組織應包括規劃、執行及日常管理人員，建議分為「風險審查與推動小組」，負責規範與審查，且其成員位階不宜過低，以及「風險評鑑執行小組」負責風險評鑑與處理，說明如下：

●風險審查與推動小組

– 審核風險評鑑的結果與風險處理計畫。

– 審核資通安全相關文件，如資通安全手冊、程序及指引等。

– 設小組執行秘書 1 名。

– 審查風險評鑑內容，包括風險處理計畫的風險評鑑報告。

– 審查因風險評鑑結果而需修改的資通安全相關文件。

– 根據風險評鑑報告鑑別需採取的安控機制。

●風險評鑑執行小組

– 定期執行風險評鑑。

– 檢視機關同仁所提列之資訊及資通系統資產項目及相關安控機制，並與機關內各單位(或各位同仁）討論或修改相關安控機制。

– 針對提列的資訊及資通系統資產項目鑑別其價值與安全需求，並分析安控機制之實施狀況。

– 盤點與鑑別各單位之資訊及資通系統資產價值。

– 鑑別潛在風險與提出需求。

– 彙總機關內各單位(或各同仁)的風險評鑑結果。

– 撰寫風險評鑑報告。

– 與風險審查與推動小組執行秘書討論風險評鑑報告，並修改其撰寫內容。

– 陳報風險評鑑報告給風險審查與推動小組召集人。

– 研議安控目標與機制，並進行安控機制之建置。

– 與風險審查與推動小組執行秘書討論並建議修復等級。

– 撰寫風險處理計畫。

– 陳報風險處理計畫給風險審查與推動小組。

– 依據風險處理計畫，實施建議之安全控制措施。

3.3 風險評鑑階段

本階段主要針對風險評鑑「建立全景階段」所定義的範疇，根據「風險評鑑程序階段」所選擇的風險評鑑循環作法，進行相對之風險評鑑作法程序實作，包括高階風險評鑑作法、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。

3.3.1 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。以「全球資訊網」為例，依表 4 範例說明「高階風險評鑑作法」進行評鑑的過程與結果(詳見圖 11)，再針對風險評估準則，定義不可接受等級之資通系統，進行風險處理計畫作業，可依據「安全控制措施參考指引」[8]，依風險等級為「普」、「中」及「高」之資通系統，執行對應之「普」、「中」及「高」控制措施。

●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。

綜整以上評定之結果，「全球資訊網」之安全等級(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：資通安全責任等級分級辦法

圖11 全球資訊網安全等級評估參考範例

3.3.2 詳細風險評鑑作法

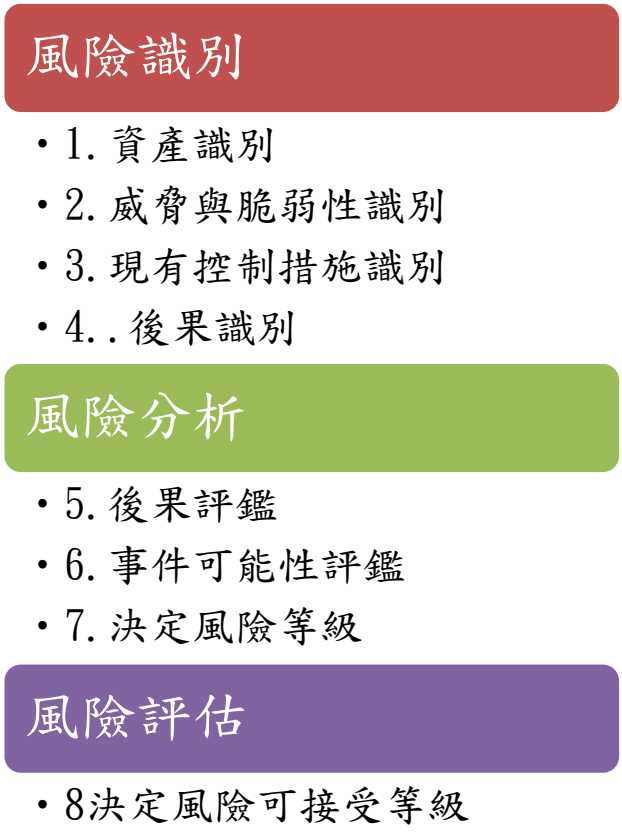
詳細風險評鑑作法乃透過系統化方式，找出該資通系統應優先處理的資訊及資通系統資產所對應的風險，而施予適當的安控措施，以維持組織持續運作。機關應參考 3.2.1 所訂定的「風險評估準則」與「衝擊準則」執行風險分析，得到所有資訊及資通系統資產的風險值；接著執行風險評估，

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 12。

得到需要執行風險處理的資訊及資通系統資產清單後，接續執行「風險處理」，並確保執行完成「風險處理」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」。

以「全球資訊網」為例，說明詳細風險評鑑作法，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)」、「評鑑事件可能性」、「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。

惟在實際作業時，「估計風險等級」與「訂定風險等級」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 個步驟說明「全球資訊網」詳細風險評鑑的執行範例。



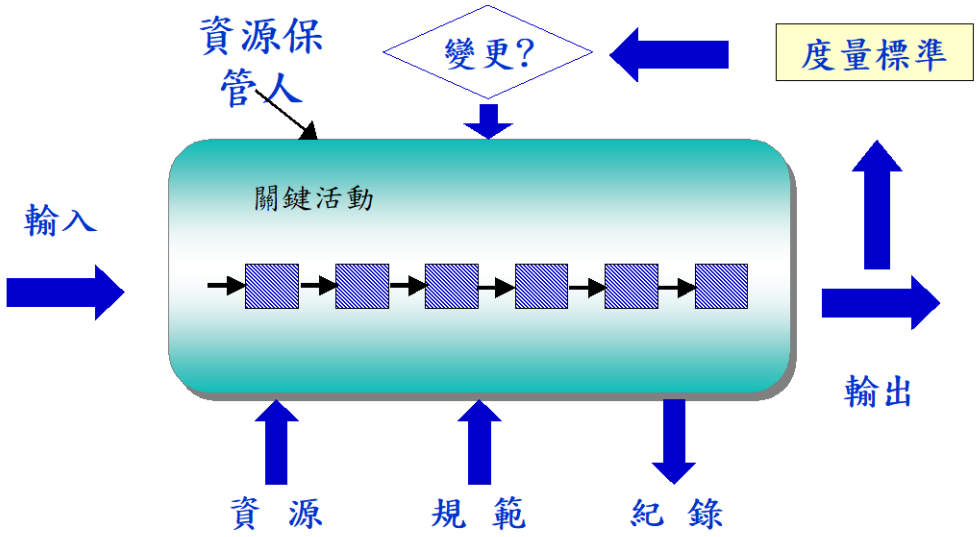
資料來源：CNS/ISO/IEC 27005:2011

圖12 詳細風險評鑑細部活動程序圖

3.3.2.1 風險識別

3.3.2.1.1 資產識別

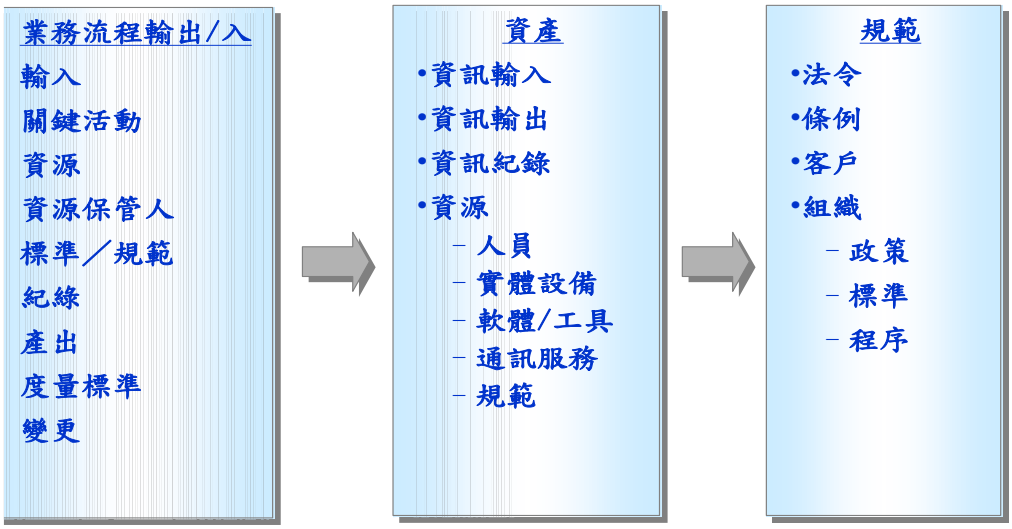
政府機關可藉由資通系統所提供的業務流程活動，識別該資通系統之資訊及資通系統資產，包括業務流程活動中之資源保管人、所需使用之資源與規範、執行關鍵活動中所產生的紀錄與最後之輸出及度量標準等，詳見圖13，均可視為「資訊及資通系統資產」。



資料來源：本計畫整理

圖13 業務流程活動示意圖

接續依據圖 13 之業務流程，條列出該業務流程之輸入與輸出，詳見圖 14，再思考這些輸出/入所代表的相關資產，即可找出可能的資訊及資通系統資產與相關規範。



資料來源：本計畫整理

圖14 識別資訊及資通系統資產程序說明圖

●範例說明

以某機關的「全球資訊網」為例，該網站說明機關成立宗旨、歷史沿革、組織結構、負責業務內容、服務範圍及最新資訊等，其業務流程的輸入/出說明如下，資產識別結果，詳見表 5。

– 輸入：「全球資訊網」所呈現的內容，如成立的宗旨、歷史沿革及組織結構等。

– 關鍵活動：新增、修改及刪除網頁內容。

– 資源與資源保管人：

➢「全球資訊網」伺服器：由「王館仁」負責管理網站。

➢「全球資訊網」系統軟體：如常見的為 Windows 200x Server 搭配 IIS，或由 Linux 搭配 Apache，本次資產識別將舉 Windows base 為例。

➢「全球資訊網」網站資料庫：MS SQL 200x。

➢「全球資訊網」網頁內容資料存放設備：本次將以一般組織常見的 NAS 設備為例，但若直接存放於伺服器上，則不必另外再鑑別出資產 NAS。

– 規範：如網站管理辦法、Win200x Server 操作暨維護手冊等。

– 紀錄：網頁內容更新與刪除申請單紀錄、伺服器及 MS SQL 200x 管理系統軌跡(logs)等。

– 輸出：網頁內容屬「資訊類別」，而資料庫 MS SQL 200x 屬「軟體類別」，兩者之威脅與脆弱性亦有不同，故應予以分別鑑別。

– 度量標準：無。

表5 「全球資訊網」資訊及資通系統資產表(範例)

NO.	部門	保管人	資產名稱	資產類別	數量	備註
1	資訊處	王館仁	全球資訊網伺服器 www.XXX.gov.tw	實體設備	1	IBM Netfinity 5xxx 系列
2	資訊處	王館仁	全球資訊網系統軟體 www.XXX.gov.tw	軟體	1	(Windows 200x Server + IIS)
3	資訊處	王館仁	MS SQL 200x 資料庫系統	軟體	1	網站資料庫軟體
4	資訊處	管姿廖	NAS 網路硬碟	實體設備	1	存放網頁內容資料
5	資訊處	管姿廖	全球資訊網網頁內容	資訊	N	存放於 NAS
6	資訊處	王管者	全球資訊網維護廠商	人員	2	XX 資訊
7	資訊處	梅仁	全球資訊網管理人員	人員	1	王館仁
8	資訊處	梅仁	NAS 管理人員	人員	1	管姿廖
9	資訊處	王館仁	網站管理辦法	資訊	1	
10	資訊處	王館仁	網站原始程式碼	資訊	N	

資料來源：本計畫整理

3.3.2.1.2 威脅與脆弱性識別

針對各項資訊及資通系統資產分別鑑別其在使用或處理過程中，各項可能的威脅運用該資訊及資通系統資產之脆弱性，對「機密性(C)」、「完整性(I)」及「可用性(A)」造成之衝擊。

當資訊及資通系統資產的威脅攻擊特定的脆弱性，而使資產受損、破壞、失能或外洩時，會對資訊及資通系統資產造成不同程度的衝擊與損失，因此依威脅與脆弱性對資訊及資通系統資產進行鑑別，以判別資訊及資通系

統資產的風險。

鑒於資訊及資通系統資產類別不同，威脅與脆弱性各有其相對應的範例，如筆記型電腦有「輕巧容易攜帶」的脆弱性，容易被「有心人士順手牽羊(威脅)」，而主機伺服器比較笨重，就不容易被「有心人士順手牽羊(威脅)」。因此，將威脅與脆弱性範例分為資訊、軟體、實體設備、服務及人員等 5 個類別(詳見附件 1)，包括「政府機關常見威脅與脆弱性範例」與「一般威脅與脆弱性範例」等。

資訊及資通系統資產的威脅識別來源，可藉由過去機關本身或其他機關曾發生的資安事件做為依據，如機關近幾年曾發生網路中斷事件，則網路中斷可視為網路設備或主機類的威脅，可檢視網路發生中斷時，機關的控制措施是否足以應對，如備援線路等，若備援線路或計畫不足，則可視為弱點。

●範例說明

針對「全球資訊網」每一項資訊及資通系統資產檢視其現況，並參考附件 1，鑑別出不同的威脅與脆弱性，同一個資訊及資通系統資產可能有一個以上的威脅與脆弱性，詳見表 6。

表6 「全球資訊網」資訊及資通系統資產威脅與脆弱性現況說明表(範例)

資訊及資通系統資產名稱	現況說明	威脅	脆弱性
全球資訊網伺服器	由於廠商維護人員更動頻繁，經常安排經驗不足人員到場維護	故障(A)	維護不當
全球資訊網系統	由於帳號未定期執行帳號審查，加上給予廠商帳號權限過大	未授權存取(C)	身分與權限設定不當

資訊及資通系統資產名稱	現況說明	威脅	脆弱性
	由於定期更新 Windows Update，恐有更新後發生異常之虞	軟體異常或錯誤(I)	定期更新或升級
MS SQL 200x 資料庫系統	由於沒有專責資料庫管理員，均委由委外廠商管理，可能留有許多未刪除之離職人員帳號或測試帳號	未授權存取(C)	身分與權限設定不當
NAS 網路硬碟	存放各系統資料，為核心系統設備	故障(A)	維護不當
全球資訊網頁內容	由於駭客技術日新月異，恐有遭置換網頁之虞	未授權變更(竄改) (I)	缺乏監控與警示機制
全球資訊網維護廠商	由於廠商開發人員眾多，並非所有人均了解委外契約中有規範「廠商所交付程式碼，不得有惡意程式碼或高風險漏洞」，且所交付程式碼經源碼檢測後，程式碼經常含許多高風險漏洞與弱點	違反合約或協議(A)	未釐清委外協議的權責
全球資訊網管理人員	負責簡單開發維護、管控網頁內容及刪除不適切帳號，偶有未依規定修改程式碼情形	未授權變更(竄改) (I)	未依照變更管理規範執行
NAS 管理人員	兼 DBA 管理人員，擁有最大存取權限	濫用(CIA)	缺乏監控與警示機制
網站管理辦法	由於操作手冊與公文管理規範均隨意放置	偷竊(CA)	缺乏存取控制機制
原始程式碼	由於原始碼存放於共用伺服器，授權資訊單位人員均可存	未授權存取(C)	缺乏存取控制機制

資訊及資通系統資產名稱	現況說明	威脅	脆弱性
	取，並未限制僅開發人員方可存取		
	同上	誤刪(IA)	缺乏刪除後的回復機制

資料來源：本計畫整理

完成「全球資訊網」資訊及資通系統資產威脅與脆弱性現況評估後，再將所識別之威脅與脆弱性進行彙總，詳見表 7。

表7 「全球資訊網」資訊及資通系統資產威脅與脆弱性對照表(範例)

NO.	部門	保管人	資產名稱	資產類別	威脅	脆弱性
1	資訊處	王館仁	全球資訊網伺服器 www.XXX.gov.tw	實體設備	故障(A)	維護不當
2	資訊處	王館仁	全球資訊網系統軟體 www.XXX.gov.tw	軟體	未授權存取(C)	身分與權限設定不當
	資訊處	王館仁	全球資訊網系統 www.XXX.gov.tw	軟體	軟體異常或錯誤(I)	定期更新或升級
3	資訊處	王館仁	MS SQL 200x 資料庫系統	軟體	未授權存取(C)	身分與權限設定不當
4	資訊處	管姿廖	NAS 網路硬碟	實體設備	故障(A)	維護不當
5	資訊處	管姿廖	全球資訊網網頁內容	資訊	未授權變更(竄改)(I)	缺乏監控與警示機制

NO.	部門	保管人	資產名稱	資產類別	威脅	脆弱性
6	資訊處	王管者	全球資訊網維護廠商	人員	違反合約或協議(A)	未釐清委外協議的權責
7	資訊處	梅仁	全球資訊網管理人員	人員	未授權變更(竄改)(I)	未依照變更管理規範 執行
8	資訊處	梅仁	NAS 管理人員	人員	濫用(CIA)	缺乏監控與警示機制
9	資訊處	王館仁	網站管理辦法	資訊	偷竊(CA)	缺乏存取控制機制
10	資訊處	王館仁	網站原始程式碼	資訊	未授權存取(C)	缺乏存取控制機制
	資訊處	王館仁	網站原始程式碼	資訊	誤刪(IA)	缺乏刪除後的回復機制

資料來源：本計畫整理

3.3.2.1.3 現有控制措施識別

了解現有控制措施之執行成效及已規劃的控制措施，再參考「安全控制措施參考指引」以確切描述安控措施，避免資源重複浪費，可透過以下方式蒐集資料：

- 檢視包含【控制措施】資訊(如風險處理計畫等)文件。
- 檢查資訊過程或資通系統中負責資安(如資安人員與資通系統安全人員與建築物管理者或營運管理者)人員與使用者所施行的【控制措施】。
- 執行實體控制的現場審查，比對已施行的及應該有的控制措施清單，並檢討已施行的控制措施是否正確與有效地運作。

●檢視內部稽核與管理階層審查結果。

●檢視矯正與預防措施結果。

●範例說明

接續針對「全球資訊網」每一項資訊及資通系統資產，找出其資產目前已實施的安全控制措施，詳見表 8。

表8 「全球資訊網」資訊及資通系統資產現有控制措施說明表(範例)

資訊及資通系統資產名稱	現有控制措施說明	安全控制措施編號
全球資訊網伺服器	定期保養維護與控管伺服器攜出機房，維護廠商庫存備品可因應設備故障，即時更換零件，另外接上 UPS 電源	11.2.1 設備安置及保護 11.2.4 設備維護 17.2.1 資訊處理設施之可用性 11.2.5 資產之攜出
全球資訊網系統軟體	每半年針對此系統執行弱點掃描，查核有無高風險漏洞之外，亦管控於 Windows 200x Server 上的軟體安裝	12.6.1 技術脆弱性管理 12.5.1 對運作中系統之軟體安裝 12.6.2 對軟體安裝之限制
MS SQL 200x 資料庫系統	啟動資料庫稽核日誌並定期審查	12.4.1 事件存錄 12.4.2 日誌資訊之保護
NAS 網路硬碟	定期作保養維護及監控 HD 容量大小	11.2.1 設備安置及保護 11.2.4 設備維護
全球資訊網網頁內容	▪定期備份與測試 ▪使用單位需填寫需求變更申請單，經主管核可，再交付資訊單位評估後，要求委外開發廠商作修改	12.3.1 資訊備份 12.4.1 事件存錄

資訊及資通系統資產名稱	現有控制措施說明	安全控制措施編號
全球資訊網維護廠商	與廠商簽訂保密協議與契約	15.1.2 於供應者協議中闡明安全性
全球資訊網管理人員	招募人員時審查資格，人事單位訂有人事管理辦法，定期宣導及辦理教育訓練	7.1.1 篩選 7.2.2 資訊安全認知、教育及訓練 7.2.3 懲處過程
NAS 管理人員	招募人員時審查資格，人事單位訂有人事管理辦法，定期宣導及辦理教育訓練	7.1.1 篩選 7.2.2 資安認知、教育及訓練 7.2.3 懲處過程
網站管理辦法	管控網站網頁內容的更新程序	12.1.1 文件化運作程序
原始程式碼	定期備份與測試並依程序變更程式碼	12.3.1 資訊備份 12.4.3 管理者及操作者日誌

資料來源：本計畫整理

再依各項資訊及資通系統資產，整理出個別的現有控制措施，詳見表 9。

表9 「全球資訊網全球資訊網」資訊及資通系統資產現有控制措施表(範例)

NO.	部門	保管人	資產名稱	資產類別	現有控制措施
1	資訊處	王館仁	全球資訊網伺服器 www.XXX.gov.tw	實體設備	11.2.1 設備安置及保護 11.2.4 設備維護 17.2.1 資訊處理設施之可用性 11.2.5 資產之攜出

NO.	部門	保管人	資產名稱	資產類別	現有控制措施
2	資訊處	王館仁	全球資訊網系統軟體 www.XXX.gov.tw	軟體	12.6.1 技術脆弱性管理 12.5.1 對運作中系統之軟體安裝 12.6.2 對軟體安裝之限制
3	資訊處	王館仁	MS SQL 200x 資料庫系統	軟體	12.4.1 事件存錄 12.4.2 日誌資訊之保護
4	資訊處	管姿廖	NAS 網路硬碟	實體設備	11.2.1 設備安置及保護 11.2.4 設備維護
5	資訊處	管姿廖	全球資訊網網頁內容	資訊	12.3.1 資訊備份 12.4.1 事件存錄
6	資訊處	王管者	全球資訊網維護廠商	人員	15.1.2 於供應者協議中闡明安全性
7	資訊處	梅仁	全球資訊網管理人員	人員	7.1.1 篩選 7.2.3 懲處過程 7.2.2 資安認知、教育及訓練
8	資訊處	梅仁	NAS 管理人員	人員	7.1.1 篩選 7.2.3 懲處過程 7.2.2 資安認知、教育及訓練
9	資訊處	王館仁	網站管理辦法	資訊	12.1.1 文件化運作程序
10	資訊處	王館仁	網站原始程式碼	資訊	12.3.1 資訊備份 12.4.3 管理者及操作者日誌

資料來源：本計畫整理

3.3.2.1.4 後果識別

後果識別乃在識別資產上可能喪失機密性、完整性及可用性之後果，換言之，每一種威脅與脆弱性結合，在不同的資訊及資通系統資產所產生的衝擊，對組織的影響是不一樣的，如電腦被植入木馬程式時，若被植入的對象是機關首長與收發人員，則其各自對組織衝擊的嚴重性不同。因此，需要識別資訊及資通系統資產發生事件後，對於組織所造成的後果。

政府機關可參考以下項目(不限於)識別事件所造成的後果：

●調查與修復時間。

●時間(工作)的損失。

●機會的損失。

●健康與安全。

●修復損害的特殊技巧之財務成本。

●形象名譽與信譽。

事件發生後，可能對資訊及資通系統資產之「機密性」、「完整性」及「可用性」造成破壞，依對組織衝擊的嚴重性描述「後果」，並依據 3.2.1 所訂定之「衝擊準則」，以「普、中、高」等 3 個等級代表後果的嚴重性，「後果識別」說明如下：

●機密性

– 普：公開資訊缺乏機密性保護，所造成後果輕微或可忽視者。

– 中：缺乏機密性保護，所造成的後果嚴重且其災害會影響業務。

– 高：缺乏機密性保護，所造成的後果很嚴重且其災害會影響業務深遠或信譽受損。

●完整性

– 普：缺乏完整性保護，所造成後果是輕微或可忽視者。

– 中：缺乏完整性保護，造成組織嚴重的後果，且其災害會影響組織業務運作。

– 高：缺乏完整性保護，造成組織很嚴重的後果，且其災害會影響組織業務停頓或信譽受損。

●可用性

– 普：缺乏可用性保護，所造成後果是輕微或可忽視者。

– 中：缺乏可用性保護，所造成的後果嚴重，且其災害會影響業務。

– 高：缺乏可用性保護，所造成的後果很嚴重，且其災害會嚴重影響業務或信譽受損。

●範例說明

當「全球資訊網」每一項資訊及資通系統資產的威脅與脆弱性鑑別完後，針對威脅與脆弱性結合而發生事件的後果予以識別，詳見表 10。

表10 「全球資訊網」後果識別(範例)

資訊及資通系統資產名稱	現況說明	後果識別描述
全球資訊網伺服器	由於廠商維護人員更動頻繁，經常安排經驗不足人員到場維護	▪若伺服器遭未授權存取，其影響可忽略，機密性評【普(1)】 ▪若伺服器遭未授權變更，恐造成伺服器中斷，完整性評【高(3)】 ▪若伺服器故障，恐造成網頁無法呈現，可用性評【高(3)】

資訊及資通系統資產名稱	現況說明	後果識別描述
		附註：本範例以全球資訊網為機關對外宣導展現機關形象的重要門面考慮，若全球資訊網並未扮演重要功能，可考量將完整性與可用性均評為【中(2)】即可
全球資訊網系統	由於帳號未定期執行帳號審查，加上給予廠商帳號權限過大	由於 Windows 200x server +IIS 安裝於伺服器上，彼此有相依的特性，可考量將資產價值與伺服器評為一致
MS SQL 200x 資料庫系統	由於沒有專責資料庫管理員，均委由委外廠商管理，可能留有許多未刪除之離職人員帳號或測試帳號	▪若 MS SQL 遭未授權變更，其影響可忽略，機密性評【普(1)】 ▪若 MS SQL 遭未授權變更，恐造成無法正確呈現網頁，影響組織，完整性評【高(3)】 ▪若 MS SQL 無法使用，恐造成無法呈現網頁，造成中斷，影響組織，可用性評【高(3)】
NAS 網路硬碟	存放各系統資料，為核心系統設備	▪由於網路硬碟不僅存放網站資料，亦存放機關核心業務系統與機敏資料，因此： ▪若網路硬碟遭未授權存取，將影響全機關，機密性評【高(3)】 ▪若網路硬碟遭未授權變更或破壞，恐造成全機關核心業務系統中斷，完整性評【高(3)】 ▪若網路硬碟故障，恐造成核心業務中斷，可用性評【高(3)】

資訊及資通系統資產名稱	現況說明	後果識別描述
全球資訊網網頁內容	由於駭客技術日新月異，恐有遭置換網頁之虞	▪若網頁內容遭未授權存取或洩密，由於均為可公開資訊，因此影響不大，機密性評【普(1)】 ▪若網頁內容遭未授權變更，將無法呈現正確網頁內容(例如：遭駭客置換網頁或置放色情圖片)，恐造成組織信譽受損，完整性評【高(3)】 ▪若網頁內容無法呈現，恐影響組織深遠，可用性評【高(3)】
全球資訊網維護廠商	由於廠商開發人員眾多，並非所有人均了解委外契約中有規範「廠商所交付程式碼，不得有惡意程式碼或高風險漏洞」，而且所交付程式碼經源碼檢測後，程式碼經常含許多高風險漏洞與弱點	▪若維護廠商洩密，由於均接觸可公開資訊，因此影響不大，機密性評【普(1)】 ▪若維護廠商作業錯誤，無法正確維護網站，將影響組織深遠，完整性評【高(3)】 ▪若維護廠商無法執行業務時，由於非經常性仰賴，影響並不大，可用性評【普(1)】
全球資訊網管理人員	負責簡單開發維護、管控網頁內容及刪除不適切帳號，偶有未依規定修改程式碼情形	▪由於管理人員均接觸可公開資訊，因此洩密影響不大，機密性評【普(1)】 ▪若管理人員作業錯誤，無法正確維護網站或放置不正確網頁內容，將影響組織深遠或信譽受損，完整性評【高(3)】 ▪若管理人員無法執行業務時，由於仰賴該員可謂不小，恐影響部門業務，可用性評【中(2)】

資訊及資通系統資產名稱	現況說明	後果識別描述
NAS 管理人員	兼 DBA 管理人員，擁有最大存取權限	▪由於 NAS 管理人員可接觸機敏資訊，因此若洩密，影響組織深遠，機密性評【高(3)】 ▪若 NAS 管理人員作業錯誤，無法正確維護 NAS，由於重要核心系統與資料均存放於此，將影響組織深遠，完整性評【高(3)】 ▪若 NAS 管理人員無法執行業務時，由於非常仰賴該員，恐影響組織業務，可用性評【高(3)】
網站管理辦法	由於操作手冊與公文管理規範均隨意放置	網站管理辦法為組織內部規範文件，遭未授權存取或修改，無法取用，均不致影響太大，均評為【普(1)】
原始程式碼	由於原始碼存放於共用伺服器，授權資訊單位人員均可存取，並未限制僅開發人員方可存取	▪原始程式碼遭未授權存取，至少影響部門業務，機密性評【中(2)】 ▪原始程式碼遭未授權修改或不正確，影響系統運作，將影響組織業務，完整性評【高(3)】 ▪原始程式碼無法使用，至少影響系統運作，將影響組織業務，完整性評【高(3)】

資料來源：本計畫整理

3.3.2.2 風險分析

3.3.2.2.1 後果評鑑(亦可視為：資訊及資通系統資產價值)

針對上述已識別相關事件情境之清單，包括對於資產及營運過程之威脅、

脆弱性及後果識別階段之輸出，評鑑可能或實際之資安事件，所導致的營運衝擊。後果識別與後果評鑑在實務上是一連續過程，只是在區分上，後果識別是整體風險識別的最後一個過程，其輸出做為後續風險分析之輸入，而後果評鑑便是風險分析的第一個過程[4]。

在評鑑後果時，應考量資產之價值，有關鑑別資訊及資通系統資產價值，可以資訊及資通系統資產在事件發生時，破壞「機密性」、「完整性」及「可用性」造成的後果，鑑別資訊及資通系統資產的價值。

資訊及資通系統資產價值評定方式包括相加、相乘、取最大值等方式，本指引範例採取最大值法，將每一資產的「機密性」、「完整性」及「可用性」代表值比較，取最大值做為資訊及資通系統資產的價值。此時不須考量是否已實施控制措施，因為鑑別資訊及資通系統資產價值，係以發生事件後對資訊及資通系統資產所造成的衝擊影響，而實施控制措施僅會影響事件發生之可能性，不會影響事件發生之衝擊程度，各類資訊及資通系統資產鑑價說明詳見附件 2。

●機密性

資訊及資通系統資產的機密性鑑價，針對資訊及其使用權限分級要求，評估其未經授權存取之影響。鑑價辦法在於資訊處理之授權，並且只有取得存取權限的人員或程序，才可進行授權範圍內之資訊處理作業。未經授權或不當的授權便進行資訊處理(包含使用設備及組織內提供之服務、執行程式、進入實體區隔之區域、透露或複製經手之業務資料)，可能對組織之業務運作造成不同程度之影響，說明如下：

– 普，其價值為 1：公開資訊缺乏機密性保護，所造成後果輕微或可忽視者。

– 中，其價值為 2：缺乏機密性保護，所造成的後果嚴重且其災害會影響業務。

– 高，其價值為 3：缺乏機密性保護，所造成的後果很嚴重且其災害會影響業務深遠或信譽受損。

另如該項資訊及資通系統資產與個人資料處理有關，請先針對該系統處理的個人資料內容進行盤點，確認其資料敏感程度，如含有財務、權益或特種資料等，應列為「高」；其他一般識別性資訊，如姓名與聯絡方式，則建議至少列為「中」，以強調個人資料保護的重要性。

●完整性

資訊及資通系統資產的完整性鑑價，針對資訊及其使用過程，必須正確地進行資訊處理的要求程度進行評估。鑑價辦法在於評估資訊與運用過程遭受變更、竄改或破壞等不當的變動或更改措施(包含移動設備、改變組織內提供之服務內容、更改系統組態或檔案、破壞實體設施、改變傳輸內容、竄改資料庫或交易資訊、冒用或假借名義進行業務處理或人為錯誤或誤用設施)，可能對組織之業務運作造成不等程度之影響，說明如下：

– 普，其價值為 1：缺乏完整性保護，所造成後果是輕微或可忽視者。

– 中，其價值為 2：缺乏完整性保護，會造成組織嚴重的後果，且其災害會影響組織業務運作。

– 高，其價值為 3：缺乏完整性保護，會造成組織很嚴重的後果，且其災害會影響組織業務停頓或信譽受損。

●可用性

資訊及資通系統資產的可用性鑑價，針對資訊與其處理過程，獲得適當授權者對於資訊與處理設備於需要存取時，能正常使用的需求程度。鑑價辦法在於評估其資訊運用過程中，提供正常服務的時間，以程度區分對不同資產之需求。影響資產可用性被破壞情況，如實體設施無法使

用、實體區域無法進入、系統軟體或程式錯誤導致執行中斷、網路連線中斷、職務代理不明或未建立相關辦法，說明如下：

– 普，其價值為 1：缺乏可用性保護，所造成後果是輕微或可忽視者。

– 中，其價值為 2：缺乏可用性保護，所造成的後果嚴重，且其災害會影響業務。

– 高，其價值為 3：缺乏可用性保護，所造成的後果很嚴重，且其災害會嚴重影響業務者或信譽受損。

當完成資訊及資通系統資產價值評鑑後，需再針對有相依關係的各項資訊及資通系統資產之「機密性」、「完整性」及「可用性」，作一致與合理化的檢視與調整，以確保有相依性之資訊及資通系統資產皆可得到相等值的保護措施。

先由「資訊」資產切入檢視與其他資訊及資通系統資產之關係，再檢視「軟體」資產為多個資通系統共用情況，最後檢視「硬體」資產為多個資通系統共用情況，說明如下：

- 當「資訊」資產的「機密性」、「完整性」及「可用性」值確定後，與此「資訊」資產相關的實體設備、軟體及人員之「機密性」、「完整性」及「可用性」值須等於或大於「資訊」資產之「機密性」、「完整性」及「可用性」值。
- 當「軟體」資產為多個資通系統共用時，檢視此「軟體」資產的「機密性」、「完整性」及「可用性」最高值，以此最高值調整其他資通系統相關的資訊、軟體、實體設備及人員之「機密性」、「完整性」及「可用性」值，須等於或大於「軟體」資產之「機密性」、「完整性」及「可用性」值。
- 「硬體」資產為多個資通系統共用時，檢視此「硬體」資產的「機密

性」、「完整性」及「可用性」最高值，以此最高值調整其他資通系統相關的資訊、軟體、實體設備及人員之「機密性」、「完整性」及「可用性」值，須等於或大於「硬體」資產之「機密性」、「完整性」及「可用性」值。

●範例說明

經後果評鑑之資產價值範例，詳見表 11。

表11 「全球資訊網」資訊及資通系統資產價值(後果評鑑)範例

資訊及資通系統資產名稱	現況說明	後果識別描述	資訊及資通系統資產價值
全球資訊網伺服器	由於廠商維護人員更動頻繁，經常安排經驗不足人員到場維護	▪若伺服器遭未授權存取，其影響可忽略，機密性評【普(1)】 ▪若伺服器遭未授權變更，恐造成伺服器中斷，完整性評【高(3)】 ▪若伺服器故障，恐造成網頁無法呈現，可用性評【高(3)】 附註：本範例以全球資訊網為機關對外宣導展現機關形象的重要門面考慮，若全球資訊網並未扮演重要功能，可考量將完整性與可用性均評為【中(2)】即可	▪機密性【普(1)】 ▪完整性【高(3)】 ▪可用性【高(3)】
全球資訊網系統	由於帳號未定期執行帳號審查，	由於 Windows 200x server +IIS 安裝於伺服	▪機密性【普(1)】

資訊及資通系統資產名稱	現況說明	後果識別描述	資訊及資通系統資產價值
	加上給予廠商帳號權限過大	器上，彼此有相依的特性，可考量將資產價值與伺服器評為一致	▪ 完整性【高(3)】 ▪ 可用性【高(3)】
MS SQL 200x 資料庫系統	由於沒有專責資料庫管理員，均委由委外廠商管理，可能留有許多未刪除之離職人員帳號或測試帳號	▪ 若 MS SQL 遭未授權變更，其影響可忽略，機密性評【普(1)】 ▪ 若 MS SQL 遭未授權變更，恐造成無法正確呈現網頁，影響組織，完整性評【高(3)】 ▪ 若 MS SQL 無法使用，恐造成無法呈現網頁，造成中斷，影響組織，可用性評【高(3)】	▪ 機密性【普(1)】 ▪ 完整性【高(3)】 ▪ 可用性【高(3)】
NAS 網路硬碟	存放各系統資料，為核心系統設備	▪ 由於網路硬碟不僅存放網站資料，亦存放機關核心業務系統與機敏資料，因此： ▪ 若網路硬碟遭未授權存取，將影響全機關，機密性評【高(3)】 ▪ 若網路硬碟遭未授權變更或破壞，恐造成全機關核心業務系統	▪ 機密性【高(3)】 ▪ 完整性【高(3)】 ▪ 可用性【高(3)】

資訊及資通系統資產名稱	現況說明	後果識別描述	資訊及資通系統資產價值
		中斷，完整性評【高(3)】 ▪若網路硬碟故障，恐造成核心業務中斷，可用性評【高(3)】	
全球資訊網頁內容	由於駭客技術日新月異，恐有遭置換網頁之虞	▪若網頁內容遭未授權存取或洩密，由於均為可公開資訊，因此影響不大，機密性評【普(1)】 ▪若網頁內容遭未授權變更，將無法呈現正確網頁內容(例如：遭駭客置換網頁或置放色情圖片)，恐造成組織信譽受損，完整性評【高(3)】 ▪若網頁內容無法呈現，恐影響組織深遠，可用性評【高(3)】	▪機密性【普(1)】 ▪完整性【高(3)】 ▪可用性【高(3)】
全球資訊網維護廠商	由於廠商開發人員眾多，並非所有人均了解委外契約中有規範「廠商所交付程式碼，不得有惡意程式碼或高風險漏洞」，而且所交付程式碼經	▪若維護廠商洩密，由於均接觸可公開資訊，因此影響不大，機密性評【普(1)】 ▪若維護廠商作業錯誤，無法正確維護網站，將影響組織深	▪機密性【普(1)】 ▪完整性【高(3)】 ▪可用性【普(1)】

資訊及資通系統資產名稱	現況說明	後果識別描述	資訊及資通系統資產價值
	源碼檢測後，程式碼經常含許多高風險漏洞與弱點	遠，完整性評【高(3)】 ▪若維護廠商無法執行業務時，由於非經常性仰賴，影響並不大，可用性評【普(1)】	
全球資訊網管理人員	負責簡單開發維護、管控網頁內容及刪除不適切帳號，偶有未依規定修改程式碼情形	▪由於管理人員均接觸可公開資訊，因此洩密影響不大，機密性評【普(1)】 ▪若管理人員作業錯誤，無法正確維護網站或放置不正確網頁內容，將影響組織深遠或信譽受損，完整性評【高(3)】 ▪若管理人員無法執行業務時，由於仰賴該員可謂不小，恐影響部門業務，可用性評【中(2)】	▪機密性【普(1)】 ▪完整性【高(3)】 ▪可用性【中(2)】
NAS 管理人員	兼 DBA 管理人員，擁有最大存取權限	▪由於 NAS 管理人員可接觸機敏資訊，因此若洩密，影響組織深遠，機密性評【高(3)】 ▪若 NAS 管理人員作業錯誤，無法正確維護	▪機密性【高(3)】 ▪完整性【高(3)】 ▪可用性【高(3)】

資訊及資通系統資產名稱	現況說明	後果識別描述	資訊及資通系統資產價值
		NAS，由於重要核心系統與資料均存放於此，將影響組織深遠，完整性評【高(3)】 ▪ 若 NAS 管理人員無法執行業務時，由於非常仰賴該員，恐影響組織業務，可用性評【高(3)】	
網站管理辦法	由於操作手冊與公文管理規範均隨意放置	網站管理辦法為組織內部規範文件，遭未授權存取或修改，無法取用，均不致影響太大，均評為【普(1)】	▪ 機密性【普(1)】 ▪ 完整性【普(1)】 ▪ 可用性【普(1)】
原始程式碼	由於原始碼存放於共用伺服器，授權資訊單位人員均可存取，並未限制僅開發人員方可存取	▪ 原始程式碼遭未授權存取，至少影響部門業務，機密性評【中(2)】 ▪ 原始程式碼遭未授權修改或不正確，影響系統運作，將影響組織業務，完整性評【高(3)】 ▪ 原始程式碼無法使用，至少影響系統運作，將影響組織業	▪ 機密性【中(2)】 ▪ 完整性【高(3)】 ▪ 可用性【高(3)】

資訊及資通系統資產名稱	現況說明	後果識別描述	資訊及資通系統資產價值
		務，完整性評【高(3)】	

資料來源：本計畫整理

經由上述評鑑理由描述後，分別評鑑出資訊及資通系統資產之價值，並以量化之數字表示，彙整結果詳見表 12。

表12 「全球資訊網」資訊及資通系統資產價值彙整表(範例)

NO.	部門	保管人	資產名稱	資產類別	機密性(C)	完整性(I)	可用性(A)	資訊及資通系統資產價值(取最大值)
1	資訊處	王館仁	全球資訊網伺服器 www.XXX.gov.tw	實體設備	1	3	3	3
2	資訊處	王館仁	全球資訊網系統軟體 www.XXX.gov.tw	軟體	1	3	3	3
3	資訊處	王館仁	MS SQL 200x 資料庫系統	軟體	1	3	3	3
4	資訊處	管姿廖	NAS 網路硬碟	實體設備	3	3	3	3
5	資訊處	管姿廖	全球資訊網 網頁內容	資訊	1	3	3	3
6	資訊處	王管者	全球資訊網 維護廠商	人員	1	3	1	3

NO.	部門	保管人	資產名稱	資產類別	機密性(C)	完整性(I)	可用性(A)	資訊及資通系統資產價值(取最大值)
7	資訊處	梅仁	全球資訊網管理人員	人員	1	3	2	3
8	資訊處	梅仁	NAS 管理人員	人員	3	3	3	3
9	資訊處	王館仁	網站管理辦法	資訊	1	1	1	1
10	資訊處	王館仁	網站原始程式碼	資訊	2	3	3	3

資料來源：本計畫整理

3.3.2.2.2 事件可能性評鑑

事件可能性是由分析威脅發生的可能性與脆弱性被運用的難易度組合而成，給予威脅發生的可能性與脆弱性被運用的難易度（普、中、高）各一個值，分別代表「威脅等級」與「脆弱性等級」，在評鑑事件可能性時，請在現有控制措施識別完成後，考量在現有控制措施實施之下，仍會發生事件的可能性來做評鑑。

●威脅等級：威脅等級、說明及發生頻率範例，詳見表 13。

– 普，其值為 1：發生可能性低，沒發生過或不可能發生。

– 中，其值為 2：發生可能性中等，曾發生過但次數很少。

– 高，其值為 3：發生可能性高，過去經常發生。

表 13 之「說明」欄中「脆弱性被利用的難易度」、「威脅的動機或能

力」及「發生可能性」3 個因素，彼此的關係是「OR」，即取三者之最高等級。以「同仁入口網」之資訊及資通系統資產「系統使用文件」，其「脆弱性被利用的難易度」為防制脆弱性被利用的安全對策有效性；「威脅的動機或能力」為威脅來源有動機也有能力；「發生可能性」為有可能發生，則威脅等級為「中」。

表13 威脅等級範例表

等級	等級值	說明	發生頻率
普	1	▪防制脆弱性被利用的安全對策有效 ▪威脅來源缺乏動機或能力不足 ▪發生頻率低	▪事件或威脅雖然沒發生過，但有可能發生 ▪平均每年發生不到 1 次 ▪平均每月人為阻止事件或威脅發生不到 1 次
中	2	▪防制脆弱性被利用的安全對策有效 ▪威脅來源有動機也有能力 ▪有可能發生	▪平均每年可能發生 1 次以上，低於 6 次 ▪平均每月人為阻止事件或威脅發生 1~3 次
高	3	▪防制脆弱性被利用的安全對策無效 ▪威脅來源有強烈的動機與足夠的能力 ▪時常發生	▪平均每年可能發生 6 次(含)以上 ▪平均每月人為阻止事件或威脅發生超過 4 次(含)以上

資料來源：本計畫整理

●脆弱性：脆弱性等級、等級值、說明及一般分級原則範例，詳見表 14。

– 普，其值為 1：很難被利用。

– 中，其值為 2：被利用的難易度適中。

– 高，其值為 3：很容易被利用。

表14 脆弱性等級範例

等級	等級值	說明	一般分級原則
普	1	脆弱性很難被利用	▪僅限深入了解脆弱性技術，並於特定條件或環境下方能利用脆弱性 ▪不會損害資訊及資通系統資產，或是受到損害後能立即回復 ▪必須運用特殊的方法才能利用脆弱性進行攻擊 ▪威脅來源必須花費長時間(可能需一個月以上)的資料蒐集，突破各層防護，才能接觸到關鍵資訊 ▪攻擊成功：可能要 1~數個月以上 ▪可能之原因 -管理防護機制完備並落實實施(例如流程控管、存取權限、通行碼政策、變更管理、稽核及應用系統經過完整測試等皆落實進行) -資訊或處理設備的使用手冊完整或說明清晰 -使用者或管理者受過完整教育訓練，對資訊處理設備操作熟練 -使用者或管理者對資訊處理程序熟悉 -技術性防護機制完備(例如資訊採用加密保護、網路區隔並採用安全設備監控系統效能、容量及安全事件；有效管理入侵/病毒/木馬、備援線路) -可被利用的方法的技術層次高或技術不容易取得實體環境的特性(例如劃分安全區域並實施監控與出入管控、環境溫濕度控管、建築物或防護設施材質等)讓威脅源被杜絕
中	2	脆弱性被利用	▪具備了解脆弱性技術知識，方能利用脆弱性 ▪資訊及資通系統資產受到損害，且無法立即回復 ▪不需用特殊的方法就能利用脆弱性進行攻擊

等級	等級值	說明	一般分級原則
		的難易度適中	▪已實施保護的機制，威脅來源必須花費一段時間(可能是數天)進行資料蒐集始能接觸到關鍵資訊 ▪攻擊成功：可能是數天以上 ▪可能之原因 -已建立管理防護機制但未落實(例如流程控管、存取權限、通行碼政策、變更管理、稽核及應用系統測試等) -資訊或處理設備的使用手冊過於簡單或說明不詳細 -使用者或管理者雖受過教育訓練，但對資訊處理設備操作不熟練 -使用者或管理者對資訊處理程序不熟悉 -雖實施技術性防護機制(例如資訊採用加密保護、網路區隔並採用安全設備、監控系統效能、容量及安全事件;有效管理入侵/病毒/木馬、備援線路)但是設定或防護能力不足 -可被利用的方法的技術層次高但技術容易取得 -實體環境的特性(例如未劃分安全區域出入管控、環境溫濕度控管不足及建築物或防護設施材質等)讓威脅源存在
高	3	脆弱性很容易被利用	▪任何人不需具備任何能力均能有意或無意的利用脆弱性 ▪資訊及資通系統資產受到嚴重損害，影響或中斷資產相關業務運作，或導致資訊及資通系統資產消失無法復原 ▪利用簡易的方法就能利用脆弱性進行攻擊 ▪未實施保護或保護機制無效，威脅來源於短期內即可攻擊成功 ▪攻擊成功：可能是一天內到數天 ▪可能之原因

等級	等級值	說明	一般分級原則
			-管理防護機制缺乏(例如流程控管、存取權限、通行碼政策、變更管理、稽核及應用系統測試等) -缺乏資訊或處理設備的操作手冊或手冊錯誤 -使用者或管理者未受過教育訓練，或對資訊處理設備操作不熟練 -使用者或管理者對資訊處理程序不了解 -缺乏技術性防護機制(例如資訊採用加密保護、網路區隔並採用安全設備、監控系統效能、容量及安全事件；有效管理入侵/病毒/木馬、備援線路) -可被利用的方法其技術層次低且容易取得 -實體環境的特性(例如未劃分安全區域出入管控、環境溫濕度控管不足及建築物或防護設施材質等)讓威脅源持續存在

資料來源：本計畫整理

●脆弱性的評估亦可以現有控制措施是否建置或落實的程度做為參考，如

– 普，其值為 1：已確實執行現有控制措施。

– 中，其值為 2：已有控制措施，但未能完全避免。

– 高，其值為 3：尚未建立控制措施。

●範例說明

到目前為止，政府機關已鑑別出「全球資訊網」的資訊及資通系統資產、資訊及資通系統資產可能有的威脅與脆弱性、現有安控機制及發生事件之後果，且以量化值呈現「後果」，現在依現有控制措施識別完成後，考量在現有控制措施下，仍會發生事件的可能性。針對「全球資訊

網」進一步分析與評鑑，詳見表 15。

表15 「全球資訊網」資訊及資通系統資產發生事件可能性說明表(範例)

資訊及資通系統資產名稱	事件可能性描述	評鑑威脅與脆弱性發生可能性
全球資訊網伺服器	▪威脅：伺服器由於定期確實維護，因此未發生故障情形 ▪脆弱性：但維護人員經常更換，由經驗不足人員擔任，對資訊處理設備操作不熟練，故脆弱性被利用難易度適中	▪威脅等級【普(1)】 ▪脆弱性等級【中(2)】
全球資訊網系統軟體	▪威脅：未發生未授權存取情形 ▪脆弱性：但未定期審查帳號權限(已建立管理防護機制但未落實)，恐有離職帳號未刪或測試帳號存在情形	▪威脅等級【普(1)】 ▪脆弱性等級【中(2)】
全球資訊網系統軟體	▪威脅：雖定期更新 Windows Update，但未測試即作更新 ▪脆弱性：曾發生軟體錯誤異常情形(已建立管理防護機制但未落實)	▪威脅等級【中(2)】 ▪脆弱性等級【中(2)】
MS SQL 200x 資料庫系統	▪威脅：未發生未授權存取情形 ▪脆弱性：但未定期審查 SQL 帳號權限(已建立管理防護機制但未落實)，恐有離職帳號未刪或測試帳號存在情形	▪威脅等級【普(1)】 ▪脆弱性等級【中(2)】
NAS 網路硬碟	▪威脅：由於定期維護並監控，發生故障可能性低 ▪脆弱性：但維護不當(管理者對資訊處理程序不熟悉)之脆弱性仍有被利用造成故障可能	▪威脅等級【普(1)】 ▪脆弱性等級【中(2)】

資訊及資通系統資產名稱	事件可能性描述	評鑑威脅與脆弱性發生可能性
全球資訊網網頁內容	▪威脅：由於駭客技術日新月異，加上曾於技服中心攻防演練時，遭成功入侵，因此，未授權變更這威脅發生可能性不低 ▪脆弱性：由於駭客技術日新月異，加上曾於技服中心攻防演練時，遭成功入侵，加上缺乏監控網頁遭變更之警示機制，故脆弱性很容易被利用	▪威脅等級【中(2)】 ▪脆弱性等級【高(3)】
全球資訊網維護廠商	▪威脅：網站開發廠商交付程式碼，經常有前十大資安漏洞，並未達契約規範「所交付程式碼不得有惡意程式碼之要求」，因此，有違反合約之可能性 ▪脆弱性：網站開發廠商資安認知不足，交付程式碼，經常有前十大資安漏洞	▪威脅等級【中(2)】 ▪脆弱性等級【中(2)】
全球資訊網管理人員	▪威脅：由於管理人員經常接到緊急變更網頁內容之要求，未依變更程序規定，要求申請者填寫網頁異動申請單，或事後未補單；因此，未授權變更發生機率不低 ▪脆弱性：未依變更管理規範執行之脆弱性易被利用	▪威脅等級【中(2)】 ▪脆弱性等級【中(2)】
NAS 管理人員	▪威脅：由於 NAS 管理人員擁最大存取權限，且未建立監控管理者存取 log 機制，雖無實際遭濫用情形，但遭濫用可能性不可忽略	▪威脅等級【中(2)】 ▪脆弱性等級【高(3)】

資訊及資通系統資產名稱	事件可能性描述	評鑑威脅與脆弱性發生可能性
	▪脆弱性：缺乏監控與警示機制之脆弱性易被利用	
網站管理辦法	▪威脅：網站管理辦法為組織內部規範文件，雖無存取控制機制，但仍未發生遭偷竊情形 ▪脆弱性：缺乏存取控制措施之脆弱性難被利用	▪威脅等級【普(1)】 ▪脆弱性等級【普(1)】
原始程式碼	▪威脅：查看存取紀錄，並無發生「資訊單位人員經由未授權存取外洩程式碼」事件 ▪脆弱性：資訊單位均可存取「原始程式碼」，所有人均可能外洩組織所有程式碼，雖有管控「僅資訊單位人員可存取」，但脆弱性被利用的難易度適中	▪威脅等級【普(1)】 ▪脆弱性等級【中(2)】
原始程式碼	▪威脅：資訊單位人員均可存取，曾發生誤刪別人程式碼情形 ▪脆弱性：缺乏刪除後回復機制之脆弱性被利用的難易度適中	▪威脅等級【中(2)】 ▪脆弱性等級【中(2)】

資料來源：本計畫整理

依據上表之發生事件可能性描述，可彙整出「全球資訊網」資訊及資通系統資產威脅與脆弱性等級，詳見表 16。

表16 「全球資訊網」資訊及資通系統資產事件發生表(範例)

NO.	部門	保管人	資產名稱	資產類別	威脅	脆弱性	威脅等級	脆弱性等級
1	資訊處	王館仁	全球資訊網伺服器 www.XXX.gov.tw	實體設備	故障(A)	維護不當	1	2
2	資訊處	王館仁	全球資訊網系統軟體 www.XXX.gov.tw	軟體	未授權存取(C)	身分與權限設定不當	1	2
	資訊處	王館仁	全球資訊網系統軟體 www.XXX.gov.tw	軟體	軟體異常或錯誤(I)	定期更新或升級	2	2
3	資訊處	王館仁	MS SQL 200x 資料庫系統	軟體	未授權存取(C)	身分與權限設定不當	1	2
4	資訊處	管姿廖	NAS 網路硬碟	實體設備	故障(A)	維護不當	1	2
5	資訊處	管姿廖	全球資訊網網頁內容	資訊	未授權變更(竄改)(I)	缺乏監控與警示機制	2	3
6	資訊處	王管者	全球資訊網維護廠商	人員	違反合約或協議(A)	未釐清委外協議的權責	2	2
7	資訊處	梅仁	全球資訊網管理人員	人員	未授權變更(竄改)(I)	未依照變更管理規範執行	2	2
8	資訊處	梅仁	NAS 管理人員	人員	濫用(CIA)	缺乏監控與警示機制	2	3

NO.	部門	保管人	資產名稱	資產類別	威脅	脆弱性	威脅等級	脆弱性等級
9	資訊處	王館仁	網站管理辦法	資訊	偷竊(CA)	缺乏存取控制機制	1	1
10	資訊處	王館仁	網站原始程式碼	資訊	未授權存取(C)	缺乏存取控制機制	1	2
	資訊處	王館仁	網站原始程式碼	資訊	誤刪(IA)	缺乏刪除後的回復機制	2	2

資料來源：本計畫整理

3.3.2.2.3 決定風險等級

●計算風險值

計算風險值乃是將量化的資訊及資通系統資產價值、後果對組織衝擊的嚴重性及事件發生的可能性結合，計算每一個資訊及資通系統資產的風險值。

資訊及資通系統資產風險值之計算，包括資訊及資通系統資產價值及風險值之計算：

– 資訊及資通系統資產價值＝(機密性鑑價、完整性鑑價及可用性鑑價)取最大值。

– 資訊及資通系統資產風險值＝(資訊及資通系統資產價值) × 威脅發生可能性 × 脆弱性利用難易度。

完成前述 3.3.2.1.4 與 3.3.2.2.2 ，可得到「全球資訊網」每項資訊及資通系統資產的量化值，即可依據公式(資訊及資通系統資產風險值＝資訊及資通系統資產價值 × 威脅發生可能性 × 脆弱性利用難易度)，分別計算

「全球資訊網」每項資訊及資通系統資產的風險值，彙整結果詳見表17。

表17 「全球資訊網」資訊及資通系統資產風險值表(範例)

NO.	部門	保管人	資產名稱	資產類別	資訊及資通系統資產價值	威脅發生可能性	脆弱性利用難易度	風險值
1	資訊處	王館仁	全球資訊網伺服器 www.XXX.gov.tw	實體設備	3	1	2	6
2	資訊處	王館仁	全球資訊網系統軟體 www.XXX.gov.tw	軟體	3	2	2	12
	資訊處	王館仁	全球資訊網系統軟體 www.XXX.gov.tw	軟體	3	2	2	12
3	資訊處	王館仁	MS SQL 200x 資料庫系統	軟體	3	1	2	6
4	資訊處	管姿廖	NAS 網路硬碟	實體設備	3	1	2	6
5	資訊處	管姿廖	全球資訊網網頁內容	資訊	3	2	3	18
6	資訊處	王管者	全球資訊網維護廠商	人員	3	2	2	12
7	資訊處	梅仁	全球資訊網管理人員	人員	3	2	2	12
8	資訊處	梅仁	NAS 管理人員	人員	3	2	3	18
9	資訊處	王館仁	網站管理辦法	資訊	1	1	1	1
10	資訊處	王館仁	網站原始程式碼	資訊	3	1	2	6
	資訊處	王館仁	網站原始程式碼	資訊	3	2	2	12

NO.	部門	保管人	資產名稱	資產類別	資訊及資通系統資產價值	威脅發生可能性	脆弱性利用難易度	風險值

資料來源：本計畫整理

- 「區分風險等級」
  - 風險值區間範圍為 1~6 者，風險等級為「普」。
  - 風險值區間範圍為 7~12 者，風險等級為「中」。
  - 風險值區間範圍為 13~27 者，風險等級為「高」。

相對風險等級之意義說明，詳見表 18。

表18 風險等級意義說明表

等級	說明
普	業務重要性、資訊流程的策略價值及法規要求低，可最後處理
中	業務重要性、資訊流程的策略價值及法規要求中等，需在既定時間以內處理完成
高	業務重要性、資訊流程的策略價值及法規要求高，需要及時處理

資料來源：本計畫整理

在初次對資訊及資通系統資產進行詳細風險評鑑時，可能因為資安控管措施執行較少或成效不彰，導致很重要的資訊及資通系統資產之脆弱性容易被威脅所利用，如根據上述計算方式，所算出之風險值最大值將為「27」。同時，在初次對資訊及資通系統資產進行詳細風險評鑑時，會對所有資訊及資通系統資產作評鑑，可能將風險很小的資訊及資通系統資產

也納入評鑑範圍，如果根據上述計算方式則其風險最小值可能為「1」，說明如下：

風險最大值＝（機密性鑑價、 完整性鑑價、 可用性鑑價其中之一為【高】）× 威脅發生可能性【高】 × 脆弱性利用難易度【高】 ＝3 × 3 × 3 ＝ 27
風險最小值＝（機密性鑑價、 完整性鑑價、 可用性鑑價三者皆為【低】）× 威脅發生可能性【低】 × 脆弱性利用難易度【低】 ＝1 × 1 × 1 ＝ 1

如果持續實施安控措施，且高風險的資訊及資通系統資產之安全管控成效良好，則其脆弱性不容易被威脅利用，雖然其資產價值高，但因威脅與脆弱性值低，故最大風險值不會達「27」，惟可本著持續改善的精神，選擇調整風險等級之風險值區間，有效地管控原屬於高風險等級的風險後，在人力與預算許可下，逐年改善所遭遇的風險，以提升資安防護等級。

接續將表 17 所彙整風險值，依「普」「中」「高」風險區間得到「全球資訊網」每個資訊及資通系統資產的風險等級，詳見表 19。

表19 「全球資訊網」資訊及資通系統資產風險等級表(範例)

NO.	部門	保管人	資產名稱	資產類別	風險值	風險等級(處理前)
1	資訊處	王館仁	全球資訊網伺服器 www.XXX.gov.tw	實體設備	6	普
2	資訊處	王館仁	全球資訊網系統軟體 www.XXX.gov.tw	軟體	12	中
	資訊處	王館仁	全球資訊網系統軟體 www.XXX.gov.tw	軟體	12	中

NO.	部門	保管人	資產名稱	資產類別	風險值	風險等級(處理前)
3	資訊處	王館仁	MS SQL 200x 資料庫系統	軟體	6	普
4	資訊處	管姿廖	NAS 網路硬碟	實體設備	6	普
5	資訊處	管姿廖	全球資訊網網頁內容	資訊	18	高
6	資訊處	王管者	全球資訊網維護廠商	人員	12	中
7	資訊處	梅仁	全球資訊網管理人員	人員	12	中
8	資訊處	梅仁	NAS 管理人員	人員	18	高
9	資訊處	王館仁	網站管理辦法	資訊	1	普
10	資訊處	王館仁	網站原始程式碼	資訊	6	普
	資訊處	王館仁	網站原始程式碼	資訊	12	中

資料來源：本計畫整理

3.3.2.3 風險評估

風險評估作業在於決定「風險可接受水準」，依據建立前景階段所訂之「風險接受準則」，檢視資訊及資通系統資產清單，訂定組織可承受的風險等級，此階段再依其所負責任務的類別與性質、服務對象、內部資源及經費預算等因素，修正風險接受準則。

如某機關之業務服務的正確性與持續性最重要，不允許任何「便民服務」停頓或中斷超過 4 小時，因此在「完整性」與「可用性」上的要求高於「機密性」，且「便民服務」的業務持續運作措施須於 4 小時內完成。因此，在資訊及資通系統資產清單中，「完整性」與「可用性」遭破壞之資訊及資通系統資產的風險值較高，將造成系統停頓或中斷超過 4 小時者列為最優先處理部分，以確保服務之正確性與持續性。

「風險值」高於或等於【「完整性」與「可用性」遭破壞並導致「系統服務」停頓或中斷超過 4 小時】的風險值之所有資訊及資通系統資產，被視為該機關「不可承受的風險範圍」，再將機關之現有預算、資源及時間納入考量，以決定其「風險接受準則」。

●業務需求及目標

– 管控服務的正確性與持續性，以維護機關信譽。

–「便民服務」的業務持續運作措施須於 4 小時內完成。

●資源分配狀況：配合業務達「便民服務」的業務持續運作措施於 4 小時內完成之目標分配資源。

●經費預算：配合業務達「便民服務的業務持續運作措施於 4 小時內完成」之目標分配預算。

完成可接受風險等級討論後，應將風險評鑑結果摘要與可接受風險等級陳報資訊單位主管核准後，再針對不可接受等級資訊及資通系統資產進行風險處理計畫作業，選用安控措施來處理高風險資產。為提供主管充分資訊以做判斷，亦可先行規劃風險處理計畫，再將風險評鑑報告與處理計畫同時陳報主管核准。

●範例說明

由於「全球資訊網」是該機關對外服務重要的管道，其風險接受準則可為【管控「全球資訊網」服務的正確性與持續性，以維護本機關信譽】。將表 19 依照風險值大小排序(詳見表 20)，再依據風險接受準則，決定「可接受風險等級」為【風險值小於 15】，故風險值大於/等於「15」之所有資訊及資通系統資產的風險均須控管，可依據「安全控制措施參考指引」，依風險等級為「普」、「中」及「高」之資訊及資通系統資產，執行對應「普」、「中」及「高」之控制措施。

表20 「全球資訊網」資訊及資通系統資產風險等級－排序表(範例)

NO.	部門	保管人	資產名稱	資產類別	風險值	風險等級(處理前)
5	資訊處	管姿廖	全球資訊網網頁內容	資訊	18	高
8	資訊處	梅仁	NAS 管理人員	人員	18	高
2	資訊處	王館仁	全球資訊網系統軟體 www.XXX.gov.tw	軟體	12	中
	資訊處	王館仁	全球資訊網系統軟體 www.XXX.gov.tw	軟體	12	中
6	資訊處	王管者	全球資訊網維護廠商	人員	12	中
7	資訊處	梅仁	全球資訊網管理人員	人員	12	中
10	資訊處	王館仁	網站原始程式碼	資訊	12	中
1	資訊處	王館仁	全球資訊網伺服器 www.XXX.gov.tw	實體設備	6	普
3	資訊處	王館仁	MS SQL 200x 資料庫系統	軟體	6	普
4	資訊處	管姿廖	NAS 網路硬碟	實體設備	6	普
10	資訊處	王館仁	網站原始程式碼	資訊	6	普
9	資訊處	王館仁	網站管理辦法	資訊	1	普
資料來源：本計畫整理						

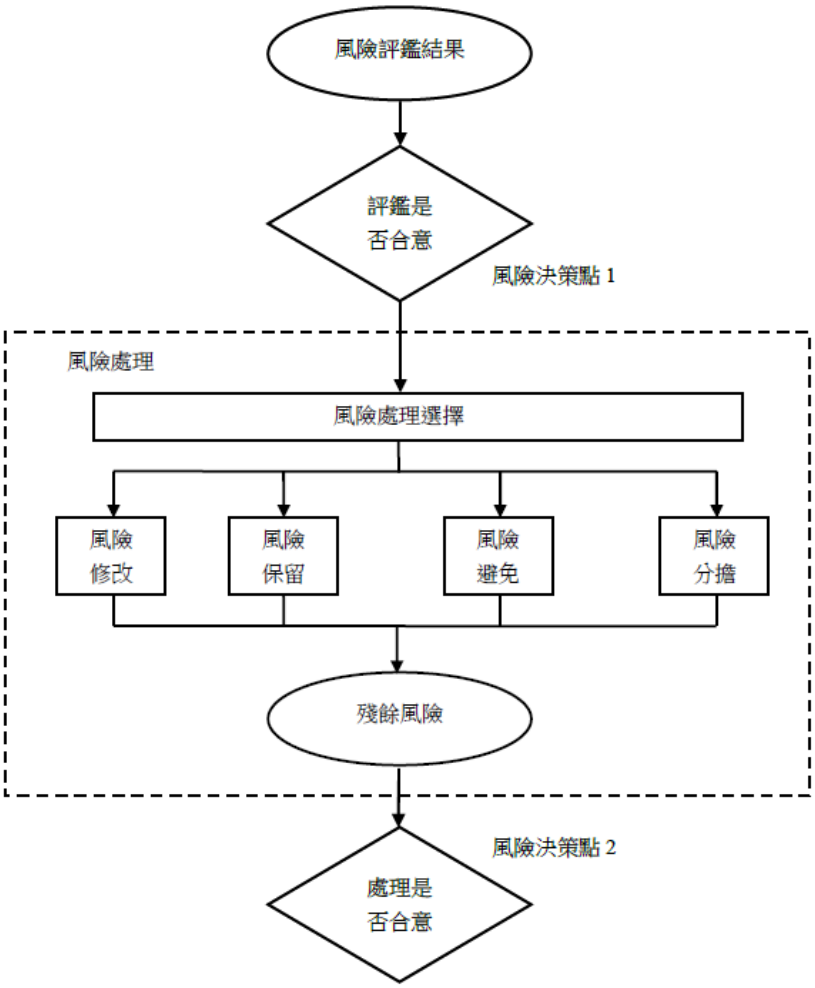
詳細風險評鑑空白表單，詳見附件 3。本指引並提供風險值計算工具暨操作手冊，詳見附件 4。

3.4 風險處理階段

風險處理活動應依風險評鑑結果及實作風險處理方案之預期成本及預期利

益等，選擇適當之行動方案，以使風險之不利後果，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 15。



資料來源：CNS 27005

圖15 風險處理活動

●風險修改(風險降低)

藉由施行、移除或改變安全控制措施，以修訂或降低風險等級，使殘餘之風險得被重新評定為可接受。

一般而言，控制措施可提供以下之一種或多種形式保護，包含矯正、消弭、預防、衝擊最小化、制止、偵測、復原、監視及認知，於控制措施選擇期間，應權衡控制措施之獲取、實作、行政管理、運作、監視及維護之成本，與受保護之資產價值加以比較。

以上風險評鑑採「高階風險評鑑作法者」，其控制措施之選擇可參考「安全控制措施參考指引」所建議之安全控制措施，依據風險評鑑之等級，分為「普」、「中」、「高」3 級，選擇適當之安全控制措施，另將控制措施施行之優先順序，區分為 P1、P2、P3 及 P0，P1 表示為應最優先施行者，P2 次之，P3 再次之，P0 則為視需要選擇項目，可依據實務需求加以選用並管理執行之優先順序。安全控制措施範例，詳見表 21。

表21 安全控制措施範例

編號	控制措施	優先順序	安全等級			控制措施內容摘要說明
			普	中	高	
Access Control 存取控制(技術類)						
AC-2	Account Management 帳號管理	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)	機關應建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序
AC-3	Access Enforcement 強制存取控制	P1	AC-3	AC-3	AC-3	作業系統應採取強制存取控制(MAC)之架構

編號	控制措施	優先順序	安全等級			控制措施內容摘要說明
			普	中	高	
AC-4	Information Flow Enforcement 資訊流強制控制	P1		AC-4	AC-4	控制資訊系統及系統間的資訊流，採強制審查授權，規範資訊在資訊系統與系統間被允許移動的路徑，以符合機關的存取控制政策
AC-5	Separation of Duties 權責分離	P1		AC-5	AC-5	採用權責分離以解決潛在濫用的授權許可，並減少共謀惡意行為的風險，包括：(i)將任務功能和資訊系統支援功能，區分到不同的使用者/角色。(ii)由不同的使用者執行資訊系統的支援功能
AC-6	Least Privilege 最小權限	P1		AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)	採用最小權限原則，只允許使用者(或代表使用者行為的程序)依據機關任務和業務功能，完成指派任務所需之授權存取
AC-17	Remote Access 遠端存取	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)	機關應對於每一種允許的遠端存取類型，都應先取得授權，建立使用限制、組態/連線需求及

編號	控制措施	優先順序	安全等級			控制措施內容摘要說明
			普	中	高	
						實作指引，並予以文件化
AC-18	Wireless Access 無線存取	P1	AC-18	AC-18 (1)	AC-18 (1) (4) (5)	機關建立無線存取資通系統應先取得授權，並建立無線存取使用限制、組態/連線需求及實作指引
AC-19	Access Control for Mobile Devices 行動裝置存取控制	P1	AC-19	AC-19 (5)	AC-19 (5)	機關資通系統對行動裝置連線應取得授權，並建立存取使用限制、組態需求、連線需求及實作指引
AC-20	Use of External Information Systems 使用外部資通系統	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)	機關應建立作業程序，以允許授權人員從外部存取機關之資通系統，或使用外部資通系統來處理、儲存或傳送機關所管控之資訊
AC-21	Information Sharing 資訊分享	P2		AC-21	AC-21	機關應在符合資訊存取限制條件下，讓授權的使用者可指派分享的存取權限
Audit and Accountability 稽核和可歸責性(技術類)						
AU-1	Audit and Accountability Policy and	P1	AU-1	AU-1	AU-1	機關應建立稽核作業程序，並定期審查與更新

編號	控制措施	優先順序	安全等級			控制措施內容摘要說明
			普	中	高	
	Procedures 稽核和可歸責性的政策和程序					
AU-2	Audit Events 稽核事件	P1	AU-2	AU-2 (3)	AU-2 (3)	機關應確保資通系統有稽核特定之事件能力，並決定有哪些特定事件在資通系統中應該被稽核
AU-3	Content of Audit Records 稽核紀錄內容	P1	AU-3	AU-3 (1)	AU-3 (1) (2)	資通系統產生的稽核紀錄至少應包含以下資訊：事件類型、何時發生、何處發生、事件來源、事件發生後的結果及任何與事件相關的使用者/主體的身分識別
AU-4	Audit Storage Capacity 稽核儲存容量	P1	AU-4	AU-4	AU-4	機關依據稽核紀錄儲存需求，配置稽核紀錄的儲存容量
AU-5	Response to Audit Processing Failures 稽核處理失效之回應	P1	AU-5	AU-5	AU-5 (1) (2)	資通系統應在稽核處理失效的情況下，警示機關特定的人員或角色，並採取額外的行動，例如：關閉資通系統、覆寫最舊的稽核紀錄或停止產生稽核紀錄等

編號	控制措施	優先順序	安全等級			控制措施內容摘要說明
			普	中	高	
AU-6	Audit Review, Analysis, and Reporting 稽核審查、分析與報告	P1	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)	機關應定期審查及分析資通系統稽核紀錄，以發現不適當或不尋常的活動，並向特定的人員或角色報告所發現的問題
AU-7	Audit Reduction and Report Generation 稽核紀錄精簡與報告產製	P2		AU-7 (1)	AU-7 (1)	機關提供稽核紀錄精簡及報表產製的功能，支援稽核審查、分析及報告之需求，以及安全事件發生後之調查，且不會改變稽核紀錄的原始內容或時間順序
AU-8	Time Stamps 時戳	P1	AU-8	AU-8 (1)	AU-8 (1)	資通系統應使用內部系統時鐘產生稽核紀錄所需時戳，並可以對映到世界協調時間(UTC)或格林威治標準時間(GMT)，並應符合機關時間測量精度的要求
AU-9	Protection of Audit Information 稽核資訊之保護	P1	AU-9	AU-9 (4)	AU-9 (2) (3) (4)	資通系統應保護稽核資訊和稽核工具，以防止未授權的存取、修改和刪除
AU-10	Non-repudiation 不可否認性	P2			AU-10	資訊系統應建立防止人員(或代表使用者行為的

編號	控制措施	優先順序	安全等級			控制措施內容摘要說明
			普	中	高	
						程序)否認曾進行機關所定義之不可否認性所涵蓋行為的防護措施
AU-11	Audit Record Retention 稽核紀錄之保存	P3	AU-11	AU-11	AU-11	機關應依律定的時間週期及紀錄留存政策要求，保留稽核紀錄，以提供及支援安全事件調查，並滿足法規和機關資訊留存需求
AU-12	Audit Generation 稽核的產生	P1	AU-12	AU-12	AU-12 (1) (3)	資訊系統應依所定義資訊系統元件中的可審核事件，提供稽核紀錄產生的能力，並允許機關特定人員或角色來選擇哪些可審核事件應被特定的資訊系統元件所稽核

資料來源：安全控制措施參考指引

●風險保留

根據風險評估結果，確認無進一步行動，而保留風險之決策。換言之，若風險等級符合風險接受準則，則不需實作額外之控制措施，該風險將被保留，惟需基於正式之決策過程。

●風險避免

風險避免係藉由從已規劃或現有活動或一組活動中退出，或變更活動運作的情況，作出完全避免風險的決定。舉例而言，對本質所引起的風險，最有成本效益的替代方案就是將該資訊處理設施實體地搬移到風險不存在或是在控制下的地點。如酒後駕車可能造成極大之後果，導致人員傷亡或是財產之重大損失，宜加以避免，故宣導開車不喝酒、喝酒不開車，便是風險避免之最佳實例。

另外，對於社交工程攻擊，除進行演練作業外，強化認知訓練及宣導，才是防範社交工程攻擊或進階持續攻擊的最有效之控制措施。

●風險分擔

依據風險評估結果，將部分之風險分擔至能有效管理該特定風險之另一方。如資訊硬體損害之風險可利用保險方案加以分擔，於重大事件發生後，可經由理賠以降低損失之程度，包含人員與資產。

或是於簽訂合約時，增訂懲罰性違約金條款，將部分之風險分擔給受委託之一方，以加強其執行風險管理之責任。

但是並非所有的風險都可經由保險之手段加以轉嫁，如對於資料資產價值之衡量便很難估計，或是因事件所造成之機關信譽損失加以補償，亦或是轉嫁之後可能導致維運成本之大幅增加。

基本上，對於硬體資產的保險方案較容易施行，除此之外，便很難用風險分擔之手段。

3.5 風險監視與審查階段

3.5.1 風險因素之監視與審查

針對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及時檢視與更新，以確保風險評鑑報告為「動態文件」。風險評鑑報告

之變更管理為當資通系統發生異動、操作的實體或網路環境改變時，用來協助識別是否需新的安全需求過程。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 16。

資料來源：本計畫整理

圖16 風險評鑑審查與變更管理時機圖

3.5.1.1 因應法律、法令、規章及合約方面要求的改變

當政府機關依其業務屬性之相對法律、法令、規章及合約方面異動時，亦將影響該機關的安全要求或安全責任，此類的異動調整與改變可能影響風險所造成的衝擊接受程度，因此應針對法律、法令、規章及合約異動影響所及的資通系統，重新檢視其風險評鑑報告。

3.5.1.2 因應資安政策的改變

當政府機關之資安政策異動時，表示管理階層重新界定安全要求或安全責任，此類的調整改變可能影響風險對於全部資通系統所造成的衝擊接受程度，因此應該針對資安政策異動影響所及的資通系統，重新檢視其風險評鑑報告。

3.5.1.3 因應環境異動

當政府機關資通系統之實體或網路環境異動時，亦將造成威脅與脆弱性的變化，實體或網路環境異動後可能發現新的威脅與脆弱性。甚至即使實體或網路環境不變，但是駭客攻擊手法與入侵技術提升時，也可能產生新的威脅與脆弱性，因此應針對環境異動影響所及的資通系統，重新檢視其風險評鑑報告。

3.5.1.4 因應資訊及資通系統資產異動

當政府機關資通系統之資訊及資通系統資產異動時，亦將造成資訊及資通系統資產本身、相關威脅與脆弱性的調整變化，如資通系統相關可能異動如下：

●新程序。

●新功能。

●軟體升級。

●硬體升級。

●包括外部群組(跨機關)或不具名群組(如民眾等)的新使用者。

●額外的「區域」或者「廣域」網路連接。

因此，應針對資訊及資通系統資產異動影響所及的資通系統，重新檢視其

風險評鑑報告，如果是「新增」資通系統，則應針對該資通系統重頭進行風險評鑑架構管理循環。

3.5.1.5 因應資安檢查結果

當政府機關因應資通系統資安弱點變化、內部資安健診(如弱點掃描、源碼檢測、社交工程演練、滲透測試或 SOC 監控等)、上級或技服中心的資安演練及技術性相關檢測，如因其檢查結果未符合資安需求與期待，或者考量所發現的新弱點或漏洞之衝擊，則應針對這些資安檢查結果影響所及的資通系統，重新檢視其風險評鑑報告。

3.5.1.6 因應資安事件的應變

政府機關資通系統如發生資安事件，則應針對資安事件影響所及的資通系統，測試檢查出在「建立全景」、「風險評鑑程序」及「執行風險評鑑」等階段中落實不夠、效度不足或需要強化之處，重新檢視調整其風險評鑑報告，並進行「矯正預防」控制措施方案。

3.5.2 內部稽核

為確保安控措施實施之有效性，定期檢視是必要的，建議每年執行 2 次內部稽核，每次稽核分為 5 個階段，依序為「準備」、「開始會議」、「稽核審查」、「結束會議」及「稽核報告」，說明如下：

●準備

– 蒐集前次內部稽核紀錄、已實施的安控機制清單及矯正與預防計畫。

– 稽核工作指派。

– 準備「內部稽核查核表」(詳見附件 5)，排定稽核日程、安排時程及通知受稽核單位安排各受檢項目之受檢人員。

●開始會議

– 說明稽核目的與範圍。

– 提供稽核方法與程序。

– 確認稽核所需的資源與設施均已備齊。

– 確認結束會議及任何中間會議的日期與時間。

●稽核審查

– 稽核人員依指派之稽核項目，以「內部稽核查核表」實施稽核，並蒐集證據將觀察事實依標準評估與記載。

– 稽核標準

➢未滿足要求、滿足小部分要求或滿足大部分要求，表示稽核項目未完全被發展、執行，列為「不符合」。

➢滿足所有要求，稽核項目完全被發展、執行，資料完整，列為「符合」。

➢這裡所描述之要求為「安全控制措施參考指引」之要求。

– 查核表列為「不符合」時，稽核人員須依觀察事實記錄在「稽核紀錄表」(詳見附件 6)，並請受稽核單位簽認。

●結束會議(Closing Meeting)

– 提報主要的觀察事實與整個稽核結論。

– 受稽核單位之主管提出評語、要求及期許。

●稽核報告

– 各稽核項目之稽核紀錄表，須由稽核人員與受稽核單位之主管簽認。

– 稽核紀錄表經簽認後複印 1 份，由稽核單位與受稽核單位分別留存，並執行矯正作業。

– 稽核完成後，建議與 2 週內，由受稽核單位提出改善措施。

– 稽核項目之缺失改善完成後，由受稽核單位通知稽核人員執行矯正行動追蹤確認。

– 稽核資料應由稽核單位與受稽核單位妥為保管。

– 透過資安稽核作業檢核狀況，進行持續改善。

3.5.3 外部稽核

透過獨立第三方執行外部稽核，也是確保安控措施實施有效性的方法。實施方式類似內部稽核，一樣要作事前的準備，聯絡外部稽核人員與通知受稽單位時程，以安排受稽人員接受稽核、參與稽核結果簡報及採取矯正與預防措施。

3.5.4 矯正預防階段

應依據「內部稽核」與「外部稽核」結果，加以「持續改進」，並針對資通系統風險評鑑不符合或需要調整改進之處，採行必要之「矯正控制措施」與「預防控制措施」，以強化與落實資通系統風險評鑑之管理成效。

3.5.4.1 持續改進

藉由資安法令法規、資安政策、內部稽核結果、外部稽核結果、監視資安事件之分析、矯正與預防控制措施並經權責主管審查，以持續且改進「風險評鑑階段」之有效性。

3.5.4.2 矯正控制措施

為防止資安事件再次發生，應決定矯正控制措施，以消除與資安管理要求不符合之原因。矯正控制措施應以文件化程序記錄備查，並包含以下事

項：

●識別各項不符合事項。

●判定各項不符合之原因。

●評估控制措施之需求，以確保各項不符合事項不復發。

●決定及實作所需之矯正控制措施。

●記錄所採取控制措施的結果。

●審查所採取之矯正控制措施。

3.5.4.3 預防控制措施

應依據「風險評鑑測試審查」管理程序，定期檢視風險評鑑控制措施的合適性與足夠性，以消除與資安管理要求「潛在不符合」之原因，並防止其發生。所採取之預防措施應與潛在問題之衝擊相對應，預防控制措施應以文件化程序記錄備查，並包含以下事項：

●識別潛在的各項不符合事項及其原因。

●評估控制措施的需求，以防止不符合事項的發生。

●決定及實作所需之預防控制措施。

●記錄所採取控制措施之結果。

●審查所採取之預防控制措施。

4. 參考文獻

[1]行政院(108 年 11 月)，資通安全責任等級分級辦法。

[2]經濟部標準檢驗局(103 年 4 月)，CNS 27001 資訊技術—安全技術—資訊安全管理系統—要求事項。

[3]International Organization for Standardization(2018 年 2 月), ISO 31000:20018 Risk management — Principles and guidelines.

[4]經濟部標準檢驗局(102 年 10 月)，CNS 27005 資訊技術—安全技術—資訊安全風險管理。

[5]行政院(109 年 9 月)，行政院及所屬各機關風險管理及危機處理作業原則。

[6]國家發展委員會(109 年 9 月)，行政院及所屬各機關風險管理及危機處理作業手冊。

[7]經濟部標準檢驗局(102 年 10 月)，CNS 31010 風險管理-風險評鑑技術。

[8]行政院資通安全辦公室(103 年 10 月)，安全控制措施參考指引(修訂)(V2.0)。

5. 附件

附件1 威脅與脆弱性範例

附件2 資訊及資通系統資產評鑑範例

附件3 詳細風險評鑑空白表單

附件4 風險值計算工具暨操作手冊

附件5 內部稽核查核表

附件6 稽核紀錄表

附件7 專有名詞英中對照表

附件8 資通系統風險評鑑參考指引導引手冊