# 1. 前言

## 1.1.目的

「資訊系統風險評鑑參考指引(修訂)」(以下簡稱本指引)旨在說明「行政院及所屬各機關資訊安全管理要點」之「各機關應依有關法令，考量施政目標，進行資訊安全風險評估，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」的內容，本指引係屬建議性質，政府機關可參考本指引，針對資訊系統與所屬資產進行風險評鑑，但不以此為限，以符合資安管理要點之要求為原則。

本指引主要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，用以評鑑機關內資訊系統的風險，以利於採取適當的安全防護控制措施，降低機關資安風險。

## 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 所示：

表1　資訊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 | *2.1* 風險的定義 | 風險的定義 | ○ | ○ | ○ | ○ |
| | *2.2* 風險安全元件 | *2.2.1* 資訊資產 | ○ | ○ | ○ | △ |
| | | *2.2.2* 威脅 | ○ | ○ | ○ | △ |
| | | *2.2.3* 脆弱性 | ○ | ○ | ○ | △ |

| 章 | 節 | 款 | 一般主管 | 資訊人員 | 資安人員 | 一般使用者 |
|---|---|---|---|---|---|---|
| 架構 | | *2.2.4* 衝擊 | ○ | ○ | ○ | △ |
| | | *2.2.5* 可能性 | ○ | ○ | ○ | △ |
| | | *2.2.6* 資訊安全模型 | ○ | ○ | ○ | △ |
| | *2.3* 資訊系統風險管理架構 | *2.3.1* 國際資訊風險管理架構 | △ | ○ | ○ | △ |
| | | *2.3.2* 我國風險管理架構 | ○ | ○ | ○ | △ |
| | *2.4* 風險評鑑作法 | *2.4.1* 高階風險評鑑作法 | △ | ○ | ○ | △ |
| | | *2.4.2* 詳細風險評鑑作法 | △ | ○ | ○ | △ |
| | | *2.4.3* 指引建議架構 | ○ | ○ | ○ | △ |
| *3* 風險評鑑管理程序 | *3.1* 建立全景階段 | *3.1.1* 風險管理基本準則 | ○ | ○ | ○ | △ |
| | | *3.1.2* 資訊系統範疇與邊界 | ○ | ○ | ○ | △ |
| | | *3.1.3* 風險評鑑組織 | ○ | ○ | ○ | △ |
| | *3.2* 風險評鑑程序階段 | *3.2.1* 風險評鑑循環程序 | ○ | ○ | ○ | |
| | | *3.2.2* 高階風險評鑑程序 | ○ | ○ | ○ | |
| | | *3.2.3* 詳細風險評鑑程序 | ○ | ○ | ○ | |
| | | *3.2.4* 既有風險評鑑程序 | ○ | ○ | ○ | |
| | *3.3* 執行風險評鑑階段 | *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」 | △ | ○ | ○ | |
| | | *3.3.3* 執行「既有風險評鑑作 | △ | ○ | ○ | |
| | *3.4* 風險評鑑測試審查階段 | *3.4.1* 風險評鑑報告審查與變更管理 | ○ | ○ | ○ | △ |
| | | *3.4.2* 內部稽核 | ○ | ○ | ○ | |
| | | *3.4.3* 外部稽核 | ○ | ○ | ○ | |
| | *3.5* 矯正預防階段 | *3.5.1* 持續改進 | ○ | ○ | ○ | |
| | | *3.5.2* 矯正控制措施 | ○ | ○ | ○ | |
| | | *3.5.3* 預防控制措施 | ○ | ○ | ○ | |

| 章 | 節 | 款 | 一般主管 | 資訊人員 | 資安人員 | 一般使用者 |
|---|---|---|---|---|---|---|
| 附記 | 各項符號代表意義說明如下：<br>○：詳閱 ； △：參考； | | | | | |

資料來源：本計畫自行整理

### 1.3.章節架構

本指引共分成前言、風險管理架構、管理程序、參考資料、網路資源表列及附件共*6* 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，引導政府機關於實施資訊系統風險評鑑時對管理目的及本指引架構能有全盤性的認知。

- 第 *2* 章「風險管理架構」首先說明風險的定義、風險安全元件(資訊資產、資訊系統、威脅、脆弱性、衝擊與可能性)、資訊安全模型，然後介紹國內外資訊系統風險管理架構以及「高階風險評鑑作法」與「詳細風險評鑑作法」等 *2* 種風險評鑑作法，最後則提出本指引建議之「風 險評鑑架構」。

- 第 *3* 章「風險評鑑管理程序」包含「建立全景階段」、風險評鑑程序 階段」、執行風險評鑑階段」、風險評鑑測試審查階段」以及「矯正預 防階段」等 *5* 大階段管理程序，描述並以「全球資訊網資訊系統」舉 例說明資訊系統風險評鑑多重循環程序。

  – 「*3.1* 建立全景階段」政府機關應該先行識別該機關內、外各方面的安 全需求以及界定風險評鑑範圍，並清查盤點該範圍內所有相關的資訊 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，最後整合這些資訊系統與資訊資

產可能涉及的跨部門業務成員，共同組成資訊系統風險評鑑組織，助於執行與落實風險評鑑的成效。

– 「*3.2* 風險評鑑程序階段」根據本指引第 *2* 章所提出的資訊系統風險評 鑑架構，以「資訊系統」爲輸入對象，並以「多重循環性」方式來實 施資訊系統之風險評鑑，本章節分別針對(*A*) 高階風險評鑑作法、(*B*) 詳細風險評鑑作法 (*C*) 機關既有風險評鑑作法等 *3* 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 該機關可運用資源之下，彈性選擇不同風險循環的組合。

– 「*3.3* 執行風險評鑑階段」根據 *3.2* 章節的 *3* 種風險評鑑程序，茲以政 府機關都擁有的「全球資訊網資訊系統」爲範例，分別說明(*A*) 高階風 險評鑑作法、(*B*) 詳細風險評鑑作法 (*C*) 機關既有風險評鑑作法等*3* 種風險評鑑作法，助於政府機關的實務操作參考。

– 「*3.4* 風險評鑑測試審查階段」程序，說明政府機關必須因應法律規章 及合約、資安政策異動、內外環境變化、資訊資產調整、資安檢查結 果與資安事故應變來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。

– 「*3.5* 矯正預防階段」程序，說明持續改進、矯正與預防控制措施。

- 第*4* 章「參考資料」詳列本指引所參考的文件或資料。
- 第*5* 章「網站資源表列」詳列本指引所參考的網站資源。
- 第*6* 章「附件」詳列本指引所納編之附件內容。

## 2. 風險管理架構

本章節首先說明風險的定義、風險安全元件(資產、威脅、脆弱性、衝擊及可能性)、資訊安全模型與風險評鑑作法(詳細風險評鑑作法與高階風險評鑑作法)，然後介紹國內外資訊系統風險管理架構，讓政府機關能瞭解資訊系統風險評鑑的相關規範、標準、演變趨勢與指引關連性。

### 2.1.風險的定義

所謂「風險(*Risk*)」乃是當「威脅(*Threat*)」利用其相對應「脆弱性(*Vulnerability*)」 直接或間接造成組織或政府機關一個或一群「資訊資產(*Asset*)」受到漏失或 損害的「可能性」。風險主要運用*2* 個因素的結合來定義其特性，分別爲「可 能性」以及其「衝擊(*Impact*)」。如能愈早偵測出資訊環境或資訊系統中變化 之資訊，將愈能增加採取適當風險處理機制來降低風險的機會，後續章節 將針對風險安全元件進行說明。

### 2.2.風險安全元件

#### 2.2.1. 資訊資產

參考*ISO*/ *IEC 27002:2005* (*CNS 27002*) 資訊安全管理之作業規範，資產乃是對 組織有價值的任何事物，組織的「資訊資產」有許多型式，如下所示：

- 資訊：資料庫及資料檔案、契約與協議、系統文件、研究資訊、使用者手冊、訓練教材、運作及支援程序、營運持續計畫、後撤(*Fallback*)安排、稽核存底及已歸檔資訊等。
- 軟體資產：應用軟體、系統軟體、開發工具及公用程式。
- 實體資產：電腦設備、通訊設備、可移除式媒體及其他設備。
- 服務：計算與通信服務、一般公用設施，例如：暖氣、照明設備、電源

及空調。

- 人員：資格、技能及經驗。
- 無形資產：例如商譽與企業形象。

但是根據 *ISO/IEC 27001*(*CNS 27001*) 在政府機關推行多年的實務經驗，本指引建議將「資訊資產」型式以下列分類較爲合適，政府機關可以根據該機關特性選擇適切分類：

- 資訊：同上
- 軟體：同上「軟體資產」
- 實體設備：同上「實體資產」
- 服務：同上
- 人員：同上

鑑於上述資訊資產與政府機關施政業務密切相關而產生價值，所以需要某種程度的資安防護，助於確保政府機關的安全需求。

### 2.2.2. 威脅

威脅乃利用資訊資產既有存在的脆弱性，以便成功地造成資訊資產的傷害或者損失，例如：未經授權的入侵、揭露、修改、毀壞造成資訊無法使用或損失。威脅可能是「環境(天然)」或「人爲」因素，而人爲因素中可以在細分爲「意外」或「故意」兩種狀況。政府機關對於意外與故意等兩種人爲因素之威脅，都應該加以識別，並評估其衝擊以及可能性，茲將威脅舉例說明，詳見表2 所示。

表2　威脅之範例

| 人爲 | | 環境(天然) |
|---|---|---|
| 故意 | 意外 | |
| ▪ 竊聽<br>▪ 資訊竄改<br>▪ 駭客侵入<br>▪ 惡意程式(木馬、病毒)<br>▪ 竊盜 | ▪ 錯誤和疏忽<br>▪ 檔案刪除<br>▪ 不正確的路由(*Routing*)<br>▪ 實體的意外 | ▪ 地震<br>▪ 閃電<br>▪ 水災<br>▪ 火災 |

資料來源：資安事故應變作業參考指引

### 2.2.3. 脆弱性

「脆弱性」是指資訊資產先天具備的特質，但卻可能會被威脅所利用而造成資訊系統或機關營運的衝擊傷害。脆弱性本身並不會造成衝擊傷害，只是讓威脅衝擊資訊資產的一個或一組條件。因此脆弱性爲先天不良，所以可能「持續」存在，除非該資訊資產本質有所改變，才有可能導致脆弱性不再出現，例如：筆記型電腦的「輕薄短小」對於小偷威脅而言，便是一個本質很難改變的脆弱性。

### 2.2.4. 衝擊

所謂「衝擊」乃是天然因素或者人爲因素中「故意」或「意外」所導致機關「非預期」的資安事故結果，此結果會影響到資訊資產，例如：資訊資產的毀滅、資訊系統的損害或者失去「機密性」、「完整性」、「可用性」、「可 歸責性」、「鑑別性」或「可靠性」。另外也可能間接影響財務收入、市場占

有率或機關形象的損失。風險衝擊的分析評估對於資訊系統風險評鑑和相

對安全防護措施的選擇乃是非常重要的判斷元素，可採用「定量」或者「定性」方式來進行風險衝擊的衡量，例如：

- 量化財務損失或者成本。
- 指定嚴重程度的經驗尺度，例如：從*1* 到*10*。
- 從預先定義的表列中選出使用的分類等級，例如：低、中、高。
- 「資訊系統分類分級與鑑別機制參考手冊」中六大構面的「普(*1*)、中(*2*)、高(*3*)」分類分級。
  - 行政院國家資通安全會報依據 *98*/*11*/*9* 行政院核定「國家資通訊安全發展 方案(*98* 年至 *101* 年)」辦理「資訊系統分類分級與鑑別機制參考手冊」，其中建議政府機關業務承辦人依「資料保護」、業務運作」、法律規章遵循」、人員傷亡」、組織信譽」及「其他」等 *6* 大構面，分別評 估對該機關各資訊系統之影響衝擊，並據以設定影響構面等級。關於「資訊系統分類分級與鑑別機制參考手冊」內容說明，將於*2.3.2.2* 章節 說明。

### 2.2.5. 可能性

風險發生的「可能性」是依據資訊資產對潛在攻擊者(威脅執行者)的誘因如何、威脅發生的可能性、以及脆弱性可被利用的難易度而定，其中威脅發生的「可能性」之影響因素如下：

- 資訊資產的價值誘惑力，當考量「故意」之人為威脅時使用。
- 資訊資產轉換成酬金的難易度，當考量「故意」之人為威脅時使用。
- 威脅起因的技術能量需求，當考量「人為威脅」時使用。
- 威脅本身發生的可能性。

- 脆弱性被利用的難易度，可考量「技術性」和「非技術性(例如：人性)」的脆弱性。

### 2.2.6. 資訊安全模型

參考 *ISO/ IEC 13335-1:2004*(*CNS 14929-1:2008*)，修訂以下的資訊安全模型，以提 供政府機關瞭解資訊安全管理議題所必要的概念，其中包含下列二個議 題，並且詳述如後續章節：

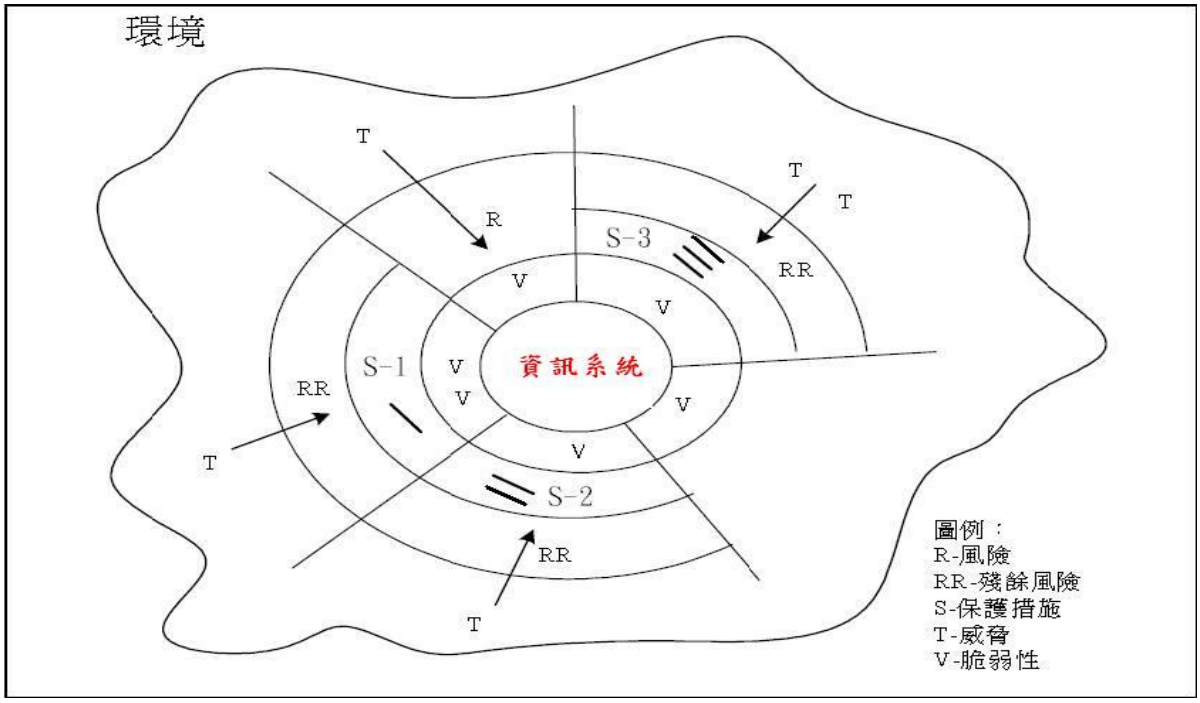
- 風險安全元件的關係。
- 風險管理的關係。

#### 2.2.6.1. 風險安全元件的關係

經觀察政府機關近年來導入 *ISMS* 之實務案例，大多採用「單一資產」之觀點，進行詳細風險評鑑，整體風險評鑑過程耗時費力，且忽略了資產與資產間的關聯性，導致相同群組之資產，卻套用不同強度之防護措施，控制措施之間出現縫隙，因而導致資安事故不斷，且往往該事故已經發生許久，卻沒有被發現，造成機敏資訊資產在不知不覺中外洩遺漏。

依據行政院文書處理手冊之文書保密規定：國家機密文書區分爲「絕對機密」「極機密」「機密」一般公務機密文書列爲「密」等級，不同等級之 機密文書合併使用或處理時，採取「最大原則」以其中「最高」之等級爲 機密等級。故當 *1* 份重要公文中含有 *3* 份附件，機密等級分別爲「普通」「密」「機密」當 *3* 份附件合併在一起時，應以「機密」文件處理，但是 當本文與附件分置時，則機密等級應該註銷。

以上之觀念也同樣適用於資訊安全之防護，故本指引參考原本 *ISO/ IEC 13335-1:2004*(*CNS 14929-1:2008*) 以「資產」爲核心之風險安全元件關係圖，修 訂爲以「資訊系統」爲核心之風險安全元件關係，詳見圖1 所示。




資料來源：本計畫自行整理

圖1　風險安全元件關係圖

上圖「資訊系統」之定義爲：負責蒐集、處理、傳送、儲存及流通資訊的一組「資產」其內容包括硬體、軟體、網路、員工、實體環境及組織架構，特別強調「資產」間之關連，並加以群組，以獲得一致的防護水準，用以協助政府機關決策、協調、控制、分析及執行。

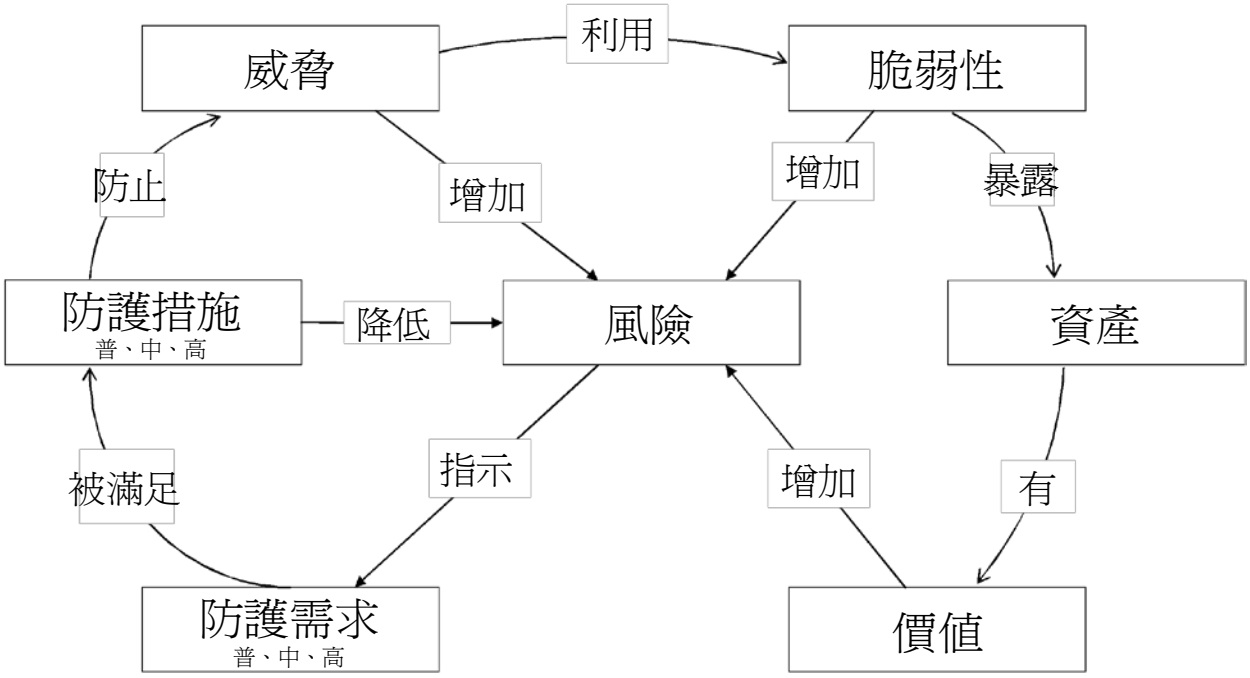
每個「資訊系統」可能存在其脆弱性，但若是無威脅可以利用該脆弱性，將不構成風險；但是如果威脅利用該資訊系統所存在之脆弱性，則可能對政府機關造成衝擊。

因此政府機關必須採取適當的「控制措施(保護措施)」藉以消弭脆弱性或者阻止威脅之利用，以降低風險；惟風險很難完全消除，務必講求成本效益，使「剩餘風險(殘餘風險)」降低至機關可接受之水準。

### 2.2.6.2. 風險管理的關係

透過以「風險」爲核心的觀點，加上「風險安全元件」彼此之間的作用關

連，可以呈現出風險管理關係圖，詳見圖2 所示。首先每個資訊系統因其所支援之施政業務活動或流程而產生其價值，當其價值愈高時，則其潛在維運的衝擊也會愈大，進而導致風險的增加。




資料來源：本計畫自行整理

圖2　風險管理關係圖

如果原本存在於資訊系統中之脆弱性遭曝露後，也會導致風險的增加，同 時如果威脅可以利用已遭曝露的脆弱性，也會增加機關之風險。

每個資訊系統的風險高低，將會引導出政府機關對該資訊系統之防護需 求，誠如前面所述，依據資安會報所制定的「資訊系統分類分級與鑑別機 制」將資訊系統安全等級區分爲「普(*1*)」、「中(*2*)」、「高(*3*)」三級，機關可 依據本指引風險評鑑後之對應防護等級需求，參考「安全控制措施參考指 引」之內容，直接選擇對應防護等級需求之普、中、高等防護措施，將可

簡化風險評鑑與風險處理的程序。

## 2.3.資訊系統風險管理架構

本章節介紹國內外資訊風險管理架構首先是美國 *NIST SP800-39* 資訊系統風險管理參考指引,該指引主要站在政府機關的整體角度來思考所欲導入「資訊系統」之風險管理架構,其架構分成 *6* 個階段,詳見表 3 所示;然後介紹 *ISO/IEC 27000* 系列中的 *ISO/IEC 27005* 資安風險管理指引,該內容則分成 *6* 個程序,同表 3 所示;最後則介紹「行政院風險管理架構」與「資訊系統分類分級與鑑別機制參考手冊」。

表3　資訊系統風險管理架構比較表

| 資訊風險管理架構 | 美國 *NIST SP800-39* | *ISO/ IEC 27005* |
|---|---|---|
| 對象/範圍 | 資訊系統 | 組織自行定義 |
| 階段/程序 | ▪ *1.*資訊與資訊系統分類分級階段<br>▪ *2.*選擇控制措施階段<br>▪ *3.*導入實施控制措施階段<br>▪ *4.*評鑑控制措施階段<br>▪ *5.*授權資訊系統上線階段<br>▪ *6.*監控應變控制措施階段 | ▪ *1.*建立全景<br>▪ *2.*風險評鑑<br>▪ *3.*風險處理<br>▪ *4.*風險接受<br>▪ *5.*風險溝通<br>▪ *6.*風險監控與審查 |

資料來源：本計畫自行整理

### 2.3.1. 國際資訊風險管理架構

#### 2.3.1.1. 美國*NIST SP800-39* 資訊系統風險管理參考指引

美國資訊安全政策從*2001* 年的*911* 事件發生之後,區分爲前後兩個時期,在 *911* 之前的時期,以電腦安全與電子商務安全爲主軸;但在*911* 之後的時期，

則著重在國土安全保護及電子化政府安全之議題上。其中*2002* 年通過「電子化政府法案(*E-Government Act*)」中的「聯邦資訊安全管理法案(*Federal Information Security Management Act*，以下簡稱 *“ FISMA”* )」即是針對資訊安全相 關推動與控制措施作強制性之要求，包括律定相關單位職掌、規範年度資 安績效稽核與評鑑、建立資安事件處理中心、發展資訊安全規範與指引等 工作。其中第 *303* 節部分更明定「國家標準與技術研究院(*National Institute of Standards and Technology,NIST*)」負責發展資訊安全相關規範與指引，並由「管 理與預算辦公室(*Office of Management and Budget, OMB*)」負責規範之推廣與督 導，經由年度的檢討作業，逐步完成資訊與資訊系統之分類、安全基準的 評估、安全機制之建置與資訊系統之認證授權等工作。*NIST* 所發表的聯邦 資訊處理標準(*Federal Information Processing Standards, FIPS*)發行系列，乃是有關 於標準和指引的官方期刊，該標準和指引在 *FISMA* 規定下被採用和執行， 其中包含 *FIPS Publication 199* 與 *FIPS Publication 200*，簡單說明如下所示：

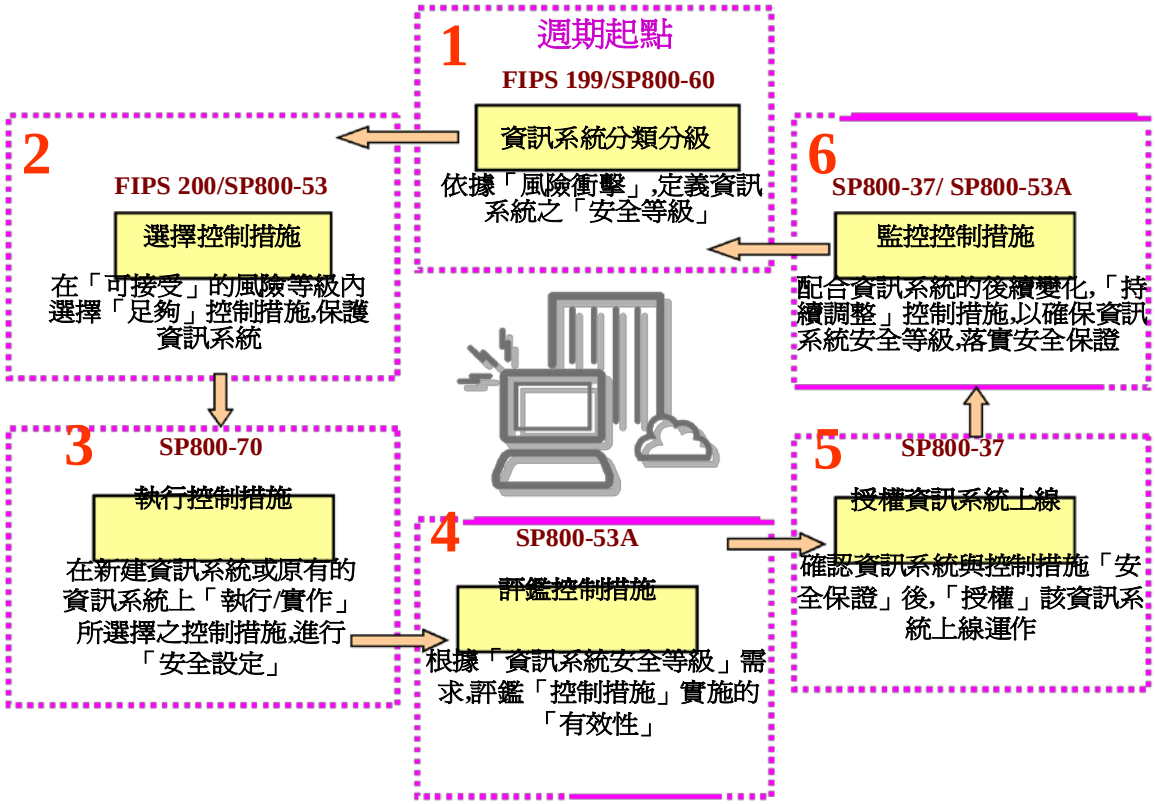
- *FIPS Publication 199* 名爲*Standards for Security Categorisation of Federal Information and Information Systems* 是*FISMA* 法案下第*1* 個強制規定的資安標準。

- *FIPS Publication 200* 名爲*Minimum Security Requirements for Federal Information and Information Systems* 則是第*2* 個強制執行的資安標準，其指出美國聯邦資訊和資訊系統就*17* 個資安領域之最低資安要求。

美國的聯邦行政機構必須選擇適當的資安控制措施來符合其單位之安全要 求，並確定該要求符合「*NIST Special Publication 800-53*(美國聯邦政府資訊系統「控制措施」建議參考指引)」以求符合該標準的最低資安要求。

*NIST SP800-39*(資訊系統之風險管理參考指引，*Managing Risk from Information Systems*)則出版於*2008* 年*4* 月，內容主要站在政府機關的整體角度來思考所 欲導入資訊系統之「風險管理架構(*Risk Management Framework,RMF*)」對於政

府機關新建資訊系統或者既有資訊系統的異動調整，皆應進行此風險管理架構來確保該資訊系統的安全等級符合該政府機關的安全需求，此架構關 鍵階段包含以下*6* 階段，詳見圖3 所示，並簡述如下所示：




資料來源： *NIST SP800-39*

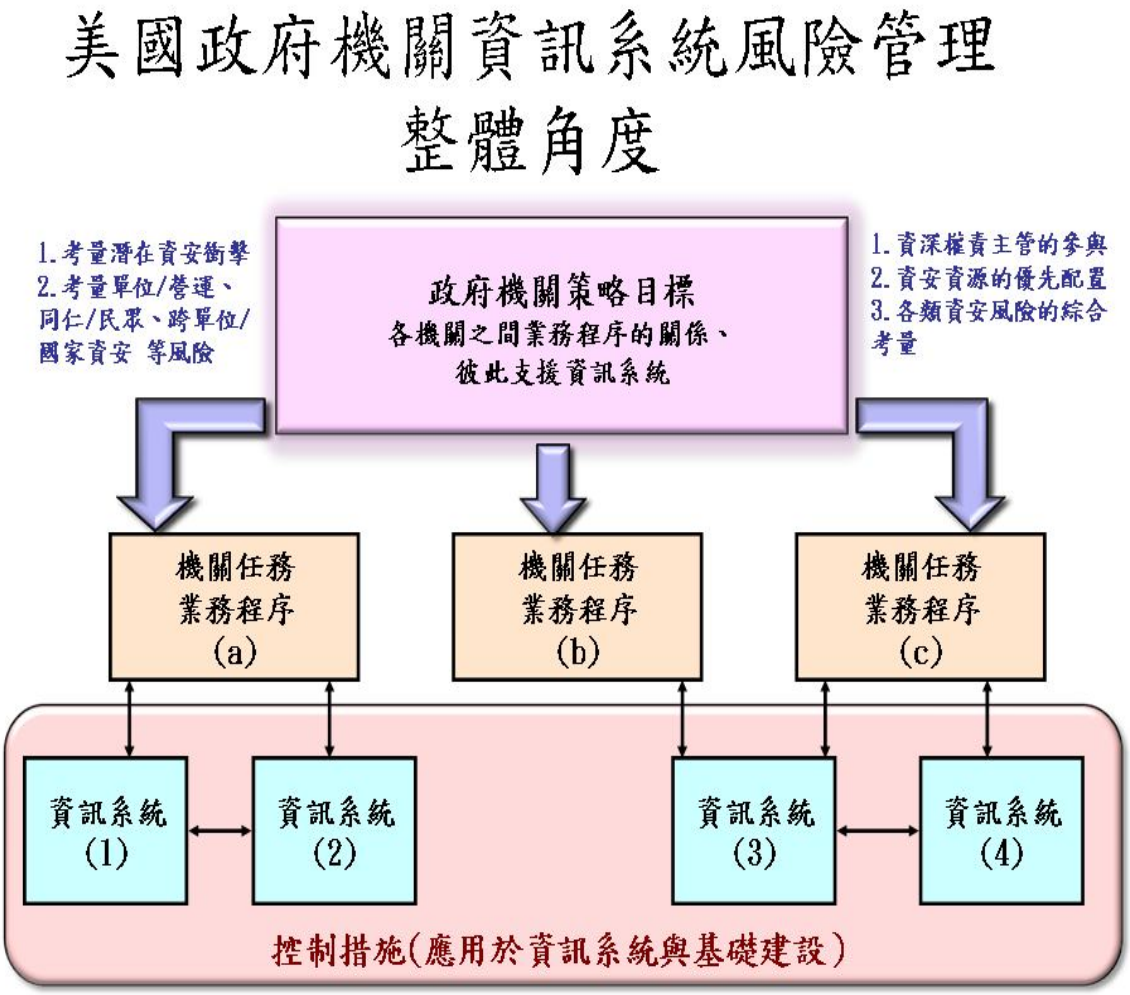
圖3 *NIST SP800-39*「資訊系統風險管理架構」

- 「*1.*資訊與資訊系統分類分級」階段
  - *NIST* 參考文件(資安標準與參考指引)： *FIPS 199*/ *NIST SP800-60*。
  - 內容重點：依據風險衝擊損失，定義資訊系統安全的分類分級。
- 「*2.*選擇控制措施」階段
  - *NIST* 參考文件(資安標準與參考指引)： *FIPS 200*/ *NIST SP800-53*。
  - 內容重點：在政府機關可接受的風險等級內選擇「足夠」數量的「控制

措施(包含：管理類、操作類與技術類)」用以保護資訊系統。

- 「*3.*導入實施控制措施」階段
  - *NIST* 參考文件(資安標準與參考指引)：*NIST SP800-70*。
  - 內容重點在新建的資訊系統或原有的資訊系統上執行控制措施並且進行安全之「設定」。
- 「*4.*評鑑控制措施」階段
  - *NIST* 參考文件(資安標準與參考指引)：*NIST SP800-53A*。
  - 內容重點：根據資訊系統安全等級需求，評鑑控制措施實施的「有效性」。
- 「*5.*授權資訊系統上線」階段
  - *NIST* 參考文件(資安標準與參考指引)：*NIST SP800-37*。
  - 內容重點：確認資訊系統與控制措施的「資訊安全保證」後，立即授權該資訊系統上線運作。
- 「*6.*監控應變控制措施」階段
  - *NIST* 參考文件(資安標準與參考指引)：*NIST SP800-37*、*NIST SP800-53A*。
  - 內容重點：配合資訊系統的後續變化，持續地調整控制措施以確保資訊系統安全等級和進一步去落實「資訊安全保證」。

*NIST SP800-39* 的發展乃是*NIST* 首先以「風險管理」與「風險評鑑」分成兩個 步驟來討論，過去「*NIST SP800-30*(資訊科技系統風險管理參考指引)」隨著 *NIST SP800-39* 的發展後已經被修訂成侷限於「風險評鑑作業」而「風險管理作業」則改以 *NIST SP800-39* 爲主，同時 *NIST SP800-39* 也說明美國政府機 關之資訊系統風險管理整體角度，詳見圖4 所示。




資料來源：*NIST SP800-39*

圖4　美國政府機關資訊系統風險管理整體角度思考圖

2.3.1.2. *ISO/IEC 27000*（*CNS 27000*）*Series* 資訊安全管理標準系列 國際標準組織將 資訊安全管理標準 統整爲*ISO/ IEC 27000*（*CNS 27000*）系列，

目前計畫發展的*ISO/ IEC 27000* 系列中主要標準之編號用途說明以及發展時程詳見表4 所示，後續章節將簡介說明 *ISO/ IEC 27001*（*CNS 27001*）、*ISO/ IEC 27002*（*CNS 27002*）與*ISO/ IEC 27005*。

表4　*ISO/ IEC 27000* (*CNS 27000*)　標準系列說明表

| 項次 | *ISO/IEC 27000* 系列號碼 | 定位用途說明 | 發展時程 |
|---|---|---|---|
| *1* | *ISO/IEC 27001* (*CNS 27001*) | *ISMS*　資訊安全管理系統-要求事項 | *2005* 年 (*2007* 年) |
| *2* | *ISO/IEC 27002* (*CNS 27002*) | *ISMS*　資訊安全管理系統-作業規範(原名*ISO 17799*) | *2005* 年 (*2007* 年) |
| *3* | *ISO/IEC 27003* | *ISMS* 導入指南 | *2010* 年 |
| *4* | *ISO/IEC 27004* | 資安管理量測標準 | *2009* 年 |
| *5* | *ISO/IEC 27005* (*CNS 27005*) | 資安風險管理指引 | *2008* 年 (*2010* 年) |
| *6* | *ISO/IEC 27006* | 國際認證政府機關對「驗證機 關」的規範 | *2007* 年 |
| *7* | *ISO/IEC 27007* | 針對*ISMS* 稽核的參考指引 | *2008* 年已完成草案 |
| *8* | *ISO/IEC 27011* | 針對通訊行業資安認證導入指 引 | *2008* 年 |
| *9* | *ISO 27799* | 針對醫療業資安認證導入指引 | *2008* 年 |

資料來源：*www.iso.org*

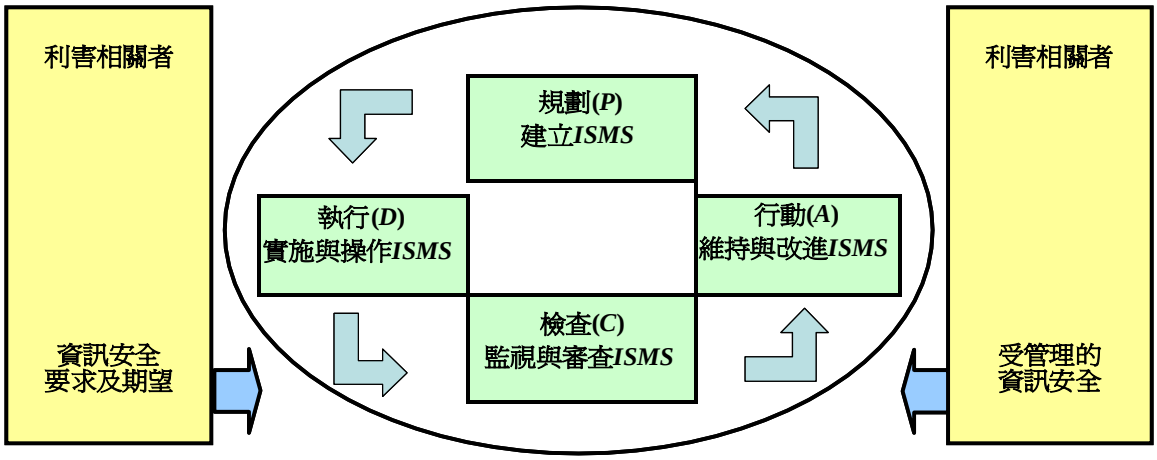
2.3.1.2.1. *ISO/ IEC 27001* (*CNS 27001*)

*ISO/ IEC 27001* (*CNS 27001*)　的目的是要制定一個用以建立、實作、運作、監控、審查、維持及改進「資訊安全管理系統」(*Information Security Management System*, *ISMS*)之模型。機關的 *ISMS* 之設計與實作受其需求與目標、安全要求、所採用的過程，以及組織之規模與架構所影響。

*ISO/ IEC 27001* (*CNS 27001*)　標準內所展現之資訊安全管理的「過程導向(作法)」鼓勵其使用者強調下列事項之重要性：

- 瞭解組織資訊安全要求，以及瞭解建立資訊安全之政策與目標的需求。
- 在組織整體營運風險之全景(*Context*)中，實作及運作各項控制措施以管理組織的資訊安全風險。
- 監控與審查*ISMS* 之績效與有效性。
- 基於客觀的測量以持續改進。

*ISO/ IEC 27001* (*CNS 27001*) 採用”規劃—執行—檢查—行動(*Plan-Do-Check-Act*, *PDCA*)”過程模型，適用於建置所有*ISMS* 過程，而有關*ISO/ IEC 27001* (*CNS 27001*) 的架構，詳見圖5 所示。




資料來源：*ISO/ IEC 27001* (*CNS 27001*)

圖5 *ISO/ IEC 27001* (*CNS 27001*) 的架構圖

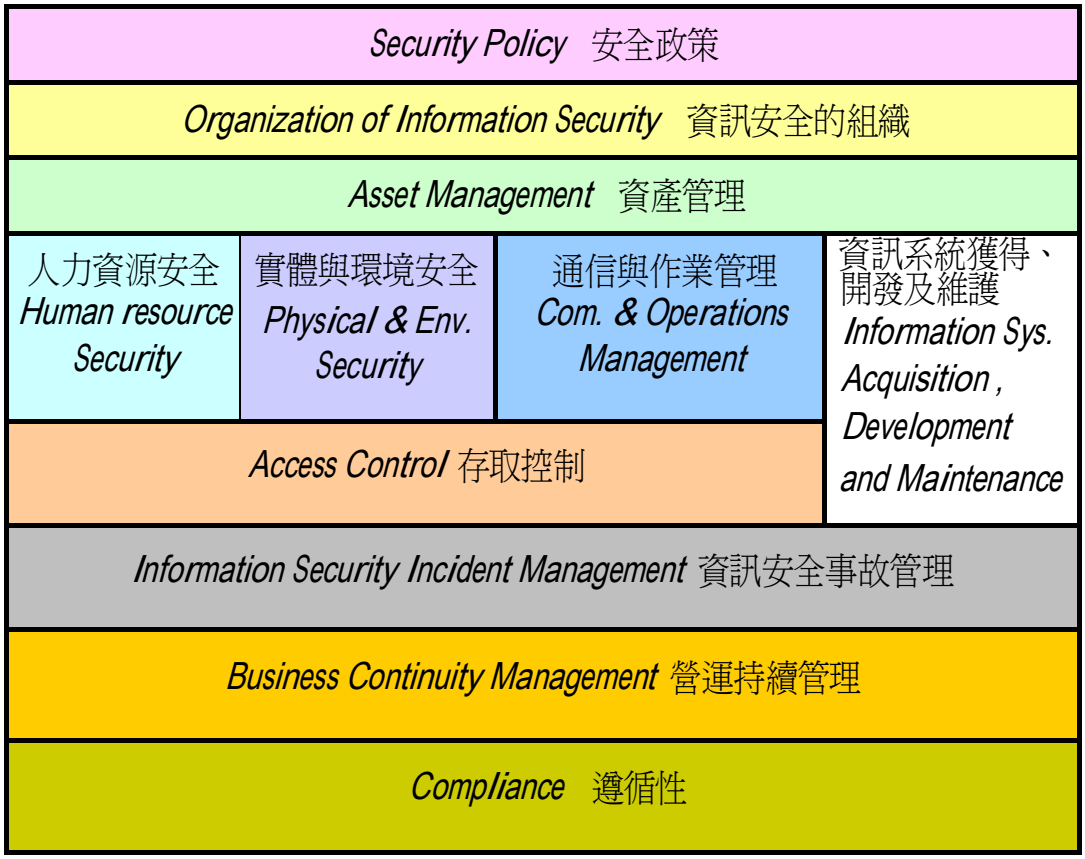
2.3.1.2.2. *ISO/IEC 27002* (*CNS 27002*)

在*2007* 年*7* 月，*ISO/IEC 17799:2005* (*CNS 17799*)正式更名爲*ISO/ IEC 27002* (*CNS 27002*)，其目的是要建立一套用以起始、實作、維持及改進組織內之資訊安全管理的指導綱要與一般原則。其控制目標與控制措施將被實作以滿足風險評鑑所識別的要求而設，可作爲發展組織安全標準及有效安全管理實務的作業指導綱要，協助建立組織間活動之信賴。

*ISO/ IEC 27002*(*CNS 27002*) 的主要內容包含如下所示：

- 「安全政策」(*Security Policy*)。
- 「資訊安全的組織」(*Organization of Information Security*)。
- 「資產管理」(*Asset Management*)。
- 「人力資源安全」(*Human Resources Security*)。
- 「實體與環境安全」(*Physical and Environmental Security*)。
- 「通信與作業管理」(*Communications and Operations Management*)。
- 「存取控制」(*Access Control*)。
- 「資訊系統獲得、開發與維護」(*Information Systems Acquisition*, *Development and Maintenance*)。
- 「資訊安全事故管理」(*Information Security Incident Management*)。
- 「營運持續管理」(*Business Continuity Management*)。
- 「遵循性」(*Compliance*)。

上述共有 *11* 個安全控制領域，其中再細分爲 *39* 個控制目標以與 *133* 個控制措施。此標準建議採用「過程導向(*Process Approach*)」的方法論，以 *PDCA* 模式，即規劃(*Plan*)、執行(*Do*)、檢查(*Check*)、行動(*Act*)，應用於組織的資訊安全工作上，以建立、實施、操作、監督、維護並持續改進組織的資訊作業安全，以管理角度爲出發點，建立與維護組織的資訊安全管理系統。而有關於*ISO/ IEC 27002*(*CNS 27002*) 的架構則詳見圖6 所示。




資料來源：*ISO/ IEC 27002*(*CNS 27002*)

圖6 *ISO/ IEC 27002*(*CNS 27002*) 的架構圖

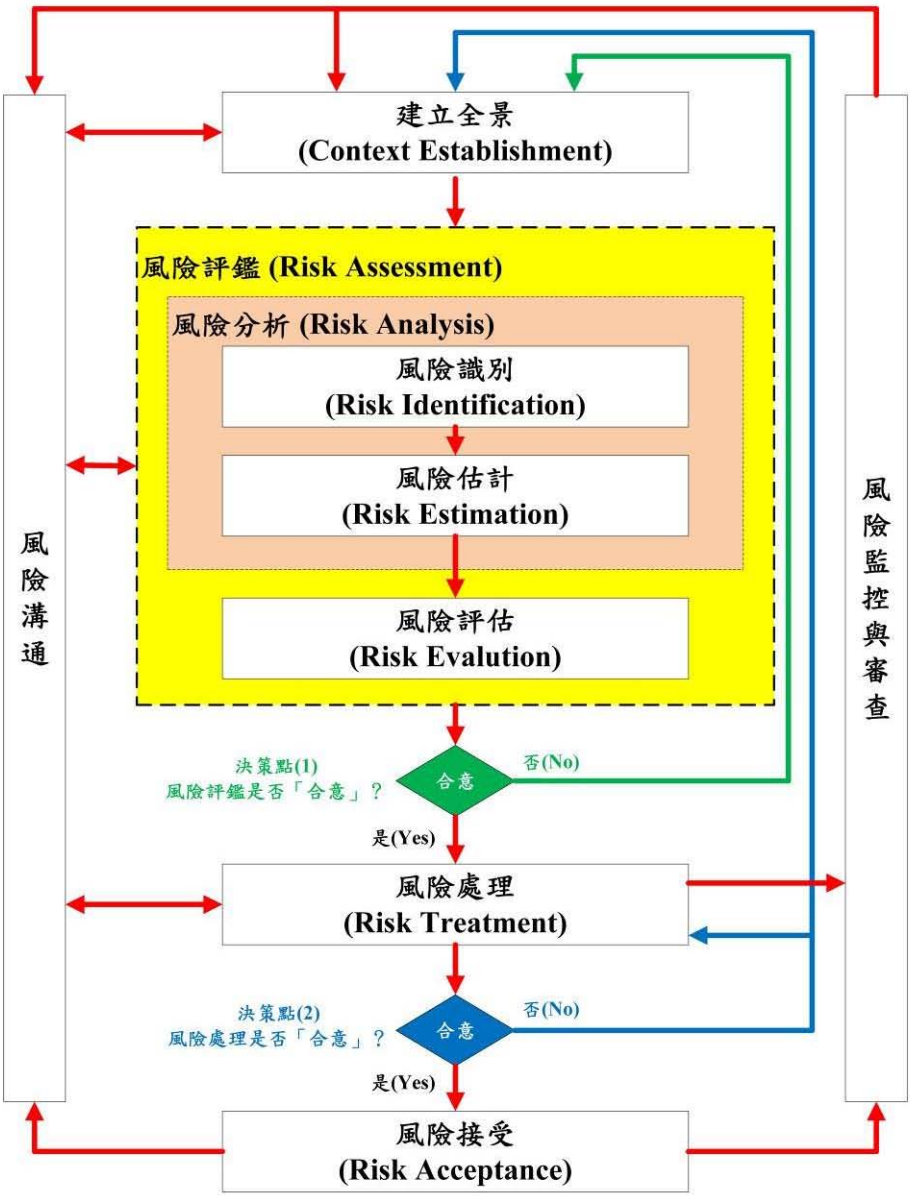
### 2.3.1.2.3. ISO/IEC 27005

*ISO/IEC 27005* 主要是在探討「資訊安全風險管理」其架構包含下列*6* 個程序，分別爲：

- 「*1.*建立全景(*Context Establishment*)」
- 「*2.*風險評鑑(*Risk Assessment*)」
- 「*3.*風險處理(*Risk Treatment*)」
- 「*4.*風險接受(*Risk Acceptance*)」
- 「*5.*風險溝通(*Risk Communication*)」

- 「*6.*風險監控與審查(*Risk Monitoring and Review*)」

至於「資訊安全風險管理」上述*6* 個程序關係，詳見圖7 所示。




資料來源：*ISO*/*IEC 27005*(中文化)

圖7　*ISO/IEC 27005* 資訊安全風險管理程序圖

*ISO/ IEC 27001*(*CNS 27001*) 規定的*ISMS* 的範圍、邊界和範疇內所實施的各項控制措施，應是基於「資安風險」的角度，而*ISO/ IEC 27005* 風險管理程序的 應用，則可以滿足這項要求。

- 在*ISMS* 中，確定範疇、風險評估、開發風險處理計畫以及風險接受都是「*1.*計畫階段(*PIan*)」中的一部分。
- 在*ISMS* 的「*2.*執行階段(*Do*)」中，按照風險處理計畫實施降低風險所需 的活動和控制措施。
- 在*ISMS* 的「*3.*檢查階段(*Check*)」管理者根據事件和環境的變化，確定 是否需要修訂風險評估和風險處理。
- 在*ISMS* 的「*4.*行動階段(*Act*)」執行任何需要的活動，包括*ISO* 風險管 理程序的補充應用。

關於*ISO/ IEC 27001*(*CNS 27001*) 的資訊安全管理系統(*ISMS*)的*PDCA* 管理程序與*ISO/ IEC 27005* 的風險管理程序之間的對照關係，詳見表5 所示。

表5 *ISMS* 與*ISO/ IEC 27005* 之資安風險管理程序對照表

| 項次 | *ISMS* 程序 | *ISO/IEC 27005* 資安風險管理程序 |
|---|---|---|
| *1* | 規劃(建立*ISMS*) | *1.*建立全景(考慮事項、基本準則、範疇、組織)<br>*2.*風險評鑑<br>*3.*發展風險處理計畫<br>*4*決定風險接受準則 |
| *2* | 執行(實作與操作*ISMS*) | *5.*實施風險處理計畫 |
| *3* | 檢查(監控與審查*ISMS*) | *6.*持續監控與審查風險 |
| *4* | 行動(維護與改進*ISMS*) | *7.*維護與改進資安風險管理程序 |

資料來源： *ISO/ IEC 27005*

### 2.3.2. 我國風險管理架構

#### 2.3.2.1. 行政院風險管理架構

*97* 年度行政院爲改善所屬各部、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。於*97*/*4*/*1* 函頒「行政院所屬各機關風險管理作業基準」

而後*97*/*12*/*8* 行政院爲進一步強化機關危機處理能量，新增納入「危機處理」專章，並配合將名稱修正爲「行政院所屬各機關風險管理及危機處理作業基準」該作業基準共分 *7* 大章節與 *27* 條準則。機關各層級參酌作業基準運作時，須設定政策目標、規劃及建置架構、執行與操作、監督審查與矯正預防及改善等作業。

建議各部會與日常運作模式相互結合，風險管理機制應整合至施政計畫各階段，建立學習型的機關，強調經驗分享，亦可善用資訊平台就跨單位跨部會議題進行資料交換、溝通與討論，以逐步累積風險辨識與評估的經驗與數據。

行政院研考會於 *98* 年 *1* 月編訂「行政院風險管理及危機處理作業手冊」以期提供行政院所屬各級機關風險管理與危機處理正確觀念、統一溝通語言及整合性架構與實務運用，有效建立風險管理與危機處理能量，順利推動並落實風險管理與危機處理，全力達成機關目標並提升施政績效與民眾滿意度。

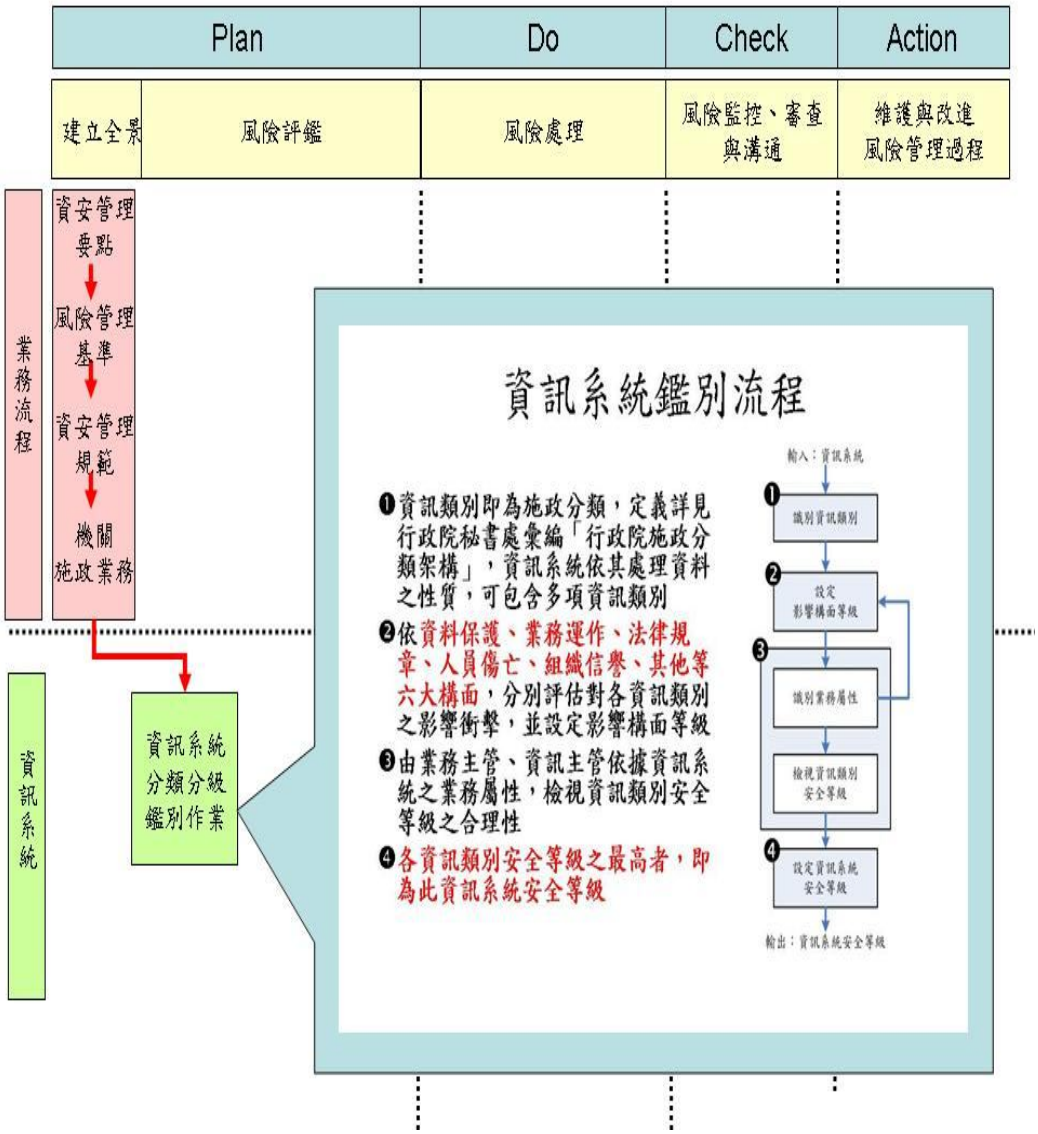
#### 2.3.2.2. 資訊系統分類分級與鑑別機制參考手冊

行政院國家資通安全會報依據*98*/*1*/*9* 行政院核定「國家資通訊安全發展方案(*98* 年至*101* 年)」辦理「資訊系統分類分級與鑑別機制參考手冊(以下簡稱“ 鑑別機制” )」鑑別機制旨在提供「資訊系統」安全等級鑑別，以協助政府

機關掌握重點保護標的，並促使機關進行風險評鑑、有效利用資源，採行適當安全控制措施，以確保各項資訊作業之安全防護水準，鑑別機制適用於各級政府機關、公營事業機構、公立研究機構、學校等之資訊系統；涉及國家機密者可參考本機制，惟仍應依「國家機密保護法」相關規定辦理。

鑑別機制處理程序中，以「資訊系統」爲輸入，其中包含❶ 識別資訊類別、❷ 設定影響構面等級、❸ 識別業務屬性並檢視安全等級 與❹設定資訊系 統安全等級 等 *4* 個處理步驟，爲說明本指引與鑑別機制的關連使用，本章 節摘錄鑑別機制部分內容，其重點步驟程序與內容，詳見圖8 與表6 所示，

各政府機關屆時參考與實作應以當時「鑑別機制」最新版本爲準。




資料來源：本計畫自行整理

圖8　資訊系統分類分級與鑑別機制處理程序

- 「資訊系統」為協助組織機關決策、協調、控制、分析及實行，負責 蒐集、處理、傳送、儲存及流通資訊的一組資產。
- ❶資訊類別即為「施政分類」行政院為推動行政資訊種類及分類標準化，以業務功能為導向，參照資訊隸屬特性及組織執掌研訂「施政分類架構」架構分為 *19* 類，包含：內政及國土安全、外交僑務及兩岸、國防及退伍軍人、財政金融、教育及體育、法務、經濟貿易、交通及建

設、勞動及人力資源、農業、衛生及社會安全、環境資源、文化及觀光、國家發展及科技、海洋事務、原住民族、客家、其他政務及輔助事務等，其定義請詳見「行政院施政分類架構知識網( *http://cake.ey.gov.tw* ) 」每個資訊系統依其處理資料之性質，可包含多項「資訊類別」

- ❷由業務承辦人依「資料保護」「業務運作」「法律規章遵循」「人員 傷亡」「組織信譽」及「其他」等六大構面，分別評估對該資訊系統各 資訊類別之影響衝擊，並據以設定影響構面等級。
- ❸由承辦單位主管依據資訊系統所屬之「行政性」「關鍵性」或「支援性」等業務屬性，檢視業務承辦人所設定資訊系統安全等級之「合理性」
- ❹該資訊系統之安全等級，需經承辦單位主管、資訊主管確認後，最後 由「資訊安全長」核定。

表6 鑑別機制處理程序之步驟說明表

| 處理步驟 | 工作項目 | 參與者 |
|---|---|---|
| 輸入<br>資訊系統 | ▪ 輸入需要鑑別「安全等級」之資訊系統 | 承辦單位主管(或其授權人員) |
| 步驟❶：識別資訊類別 | ▪ 「安全防護要求等級評估表(範本請詳見附錄 *4-1* 與 *4-3*)」之【資訊類別】欄位係參照行政 院秘書處彙編「行政院施政分類架構」之施政 分類，資訊類別取至施政分類編碼第二層爲原 則，惟機關可視需要自行調整至第三層或更多 層。<br>▪ 依系統涉及之業務範圍，由業務承辦人負責識別系統資訊所屬之資訊類別，並於【資訊類別】 | 業務承辦人 |

| 處理步驟 | 工作項目 | 參與者 |
| --- | --- | --- |
| | 欄位以「下拉式選單」依次選擇資訊類別之第一層與第二層編碼。 | |
| 步驟❷：設定影響構面等級 | ▪ 針對所選擇之各項資訊類別，由業務承辦人評估如其機密性、完整性、可用性喪失時，對「資 料護、業務運作、法律規章遵循、人員傷亡、 組織信譽及其他」等六大影響構面的衝擊程 度，並參照「安全等級設定原則」填寫影響構 面等級，等級區分爲【普、中、高】三級，分 別以【*1*、*2*、*3*】表示；對於「不適用」之影響 構面，安全等級則以【*NA*】表示。<br>▪ 各項資訊類別之安全等級即爲該資訊類別在六大影響構面等級「最高者」因此，取各列六個影響構面等級值最高者即爲該列【資訊類別安全等級】欄位值。<br>▪ 資訊系統安全等級即爲各項資訊類別安全等級「最高者」因此，取各【資訊類別安全等級】欄位值最高者即爲【資訊系統安全等級】欄位值。 | 業務承辦人 |
| 步驟❸：<br>❶識別業務屬性<br>❷檢視安全等級 | ▪ 由承辦單位主管識別資訊系統之業務屬性，並與「步驟❷：設定影響構面等級」之結果相勾稽，以檢視所設定安全等級之合理性。<br>▪ 資訊系統依其服務之業務屬性分爲【行政性業務、關鍵性業務與支援性業務】等三類，詳見[註*1*]所示。<br>▪ 資訊系統安全等級與業務屬性通常具有高度 | 承辦單位主管(或其授權人員) |

| 處理步驟 | 工作項目 | 參與者 |
| --- | --- | --- |
| | 關聯性因此可進行相互勾稽詳見[註*2*]所示。<br>▪ 本步驟所進行各項異動，均須記錄異動原因。 | |
| 步驟❹：<br>設定資訊系統安全等級 | 由資訊單位綜整各資訊系統「安全防護要求等級評估表」並製作「資訊系統清冊(參考範本，請詳見附錄 *4-2*)」，經資訊主管、各承辦單位主管確認後，最後由資訊安全長核定資訊系統安全等級。 | 資訊安全長、單位主管、資訊主管 |
| 輸出：<br>資訊系統安全等級 | 針對本程序步驟所輸入之「資訊系統」設定其「安全等級」可作爲本指引風險評鑑與選擇控制措施之依據。 | |

資料來源：資訊系統分類分級與鑑別機制參考手冊

- 【表6】之備註說明：
  - [註*1*]
    - ➢行政性業務：係指機關內部【輔助單位】之業務，若輔助單位工作 與機關職掌相同或兼具業務單位性質，機關得視情形調整業務屬性。
      - ◆ 【輔助單位】包含辦理秘書、總務、人事、主計、研考、資訊、法制、政風、公關等支援服務事項之單位，詳細定義，請參照「中央行政機關組織基準法」
    - ➢關鍵性業務：政府機關在遭遇衝擊時，須確保持續運作之「核心業務」以及與民眾生活機能相關之「關鍵基礎建設(如：水、電力、通訊電信、農產運銷、金融服務等)」均屬「關鍵性業務」
      - ◆ 【核心業務】機關應透過瞭解本身特性、目標及進行營運衝擊分析等方式，辨識機關本身之核心業務。

- ➢支援性業務：機關內部【業務單位】之業務但非列核心業務者，屬支援性業務。
  - ◆ 【業務單位】業務單位係指執行該機關職掌事項之單位，詳細定義，請參照「中央行政機關組織基準法」。

- [註*2*]
  - ➢如於【步驟❸-❶】識別業務屬性爲「關鍵性業務」，惟於【步驟❷】 設定各資訊類別安全等級卻爲「普」級(即等級*1*)。
  - ➢如於【步驟❸-❶】識別業務屬性爲「行政性業務」或「支援性業務」 惟於【步驟❷】設定部分資訊類別安全等級卻爲「高」級(即等級*3*)。
  - ➢如有上述兩種情形發生，政府機關須就其「合理性」進行確認，如確認屬實，則應於備註欄位說明原因。

鑑別機制主要在協助政府機關鑑別資訊系統安全等級、釐清重點保護標 的，後續並可供機關辦理風險評鑑及選擇安全控制措施等，影響深遠，因 此，機關每年度應針對各資訊系統至少進行*1* 次分類分級與鑑別。

另外，已通過資訊安全管理驗證(例如：*ISO/ IEC 27001*、*CNS 27001* 等)之機關， 準用已採行之風險評鑑方法，須將資訊系統衝擊評估結果轉換爲本機制之【普(*1*)、中(*2*)、高(*3*)】*3* 個安全等級。

## 2.4.風險評鑑作法

在 *ISO/ IEC 27005:2008* 內容中說明組織自行可以根據其風險評鑑目標來選擇 其風險評鑑作法，同時在其【附錄 *E*】內容中舉例說明「高階風險評鑑作 法」與「詳細風險評鑑」兩種作法，其中每種作法各有其特色、適用狀況 與注意事項，將於後續章節進行說明。

同時從圖9 中可以發現*ISO/ IEC 27005:2008* 的風險管理架構有兩個「決策點

(*Decision Point*)」一個在「風險評鑑」之後，一個在「風險處理」之後，茲分別說明如下：

- 風險評鑑決策點

此決策點讓組織可以依據其所選擇之風險評鑑方法所獲得的風險評鑑結果進行「是否合意」的判斷與決策：

– 如果「合意」則結束「風險評鑑」階段，直接進入「風險處理」階段。

– 如果「不合意」則重新進入「建立全景」階段，開始另一個風險管理 循環。此時組織亦可選擇與上個循環相同或者不同的風險評鑑作法， 重新進行「風險評鑑」直到風險評鑑結果「合意」爲止，方才進入「風 險處理」階段。

通常組織會執行兩個(或者更多)之風險評鑑循環，舉例說明如下：

– 針對某個資訊系統，第一循環執行「高階風險評鑑作法」結果爲「高風 險」爲求謹慎與正確風險處理方向，如果組織各種資源足夠，建議第 二循環得運用「詳細風險評鑑作法」來分析瞭解該資訊系統中真正關 鍵資訊資產，助於後續風險處理的正確性與有效性。

– 針對某個資訊系統，第一循環執行「高階風險評鑑作法」但其結果「不 合意」或者擔憂評鑑深度不夠而導致風險處理不夠完善，第二循環則 進行「詳細風險評鑑作法」或者「其他」適切的風險評鑑方法。

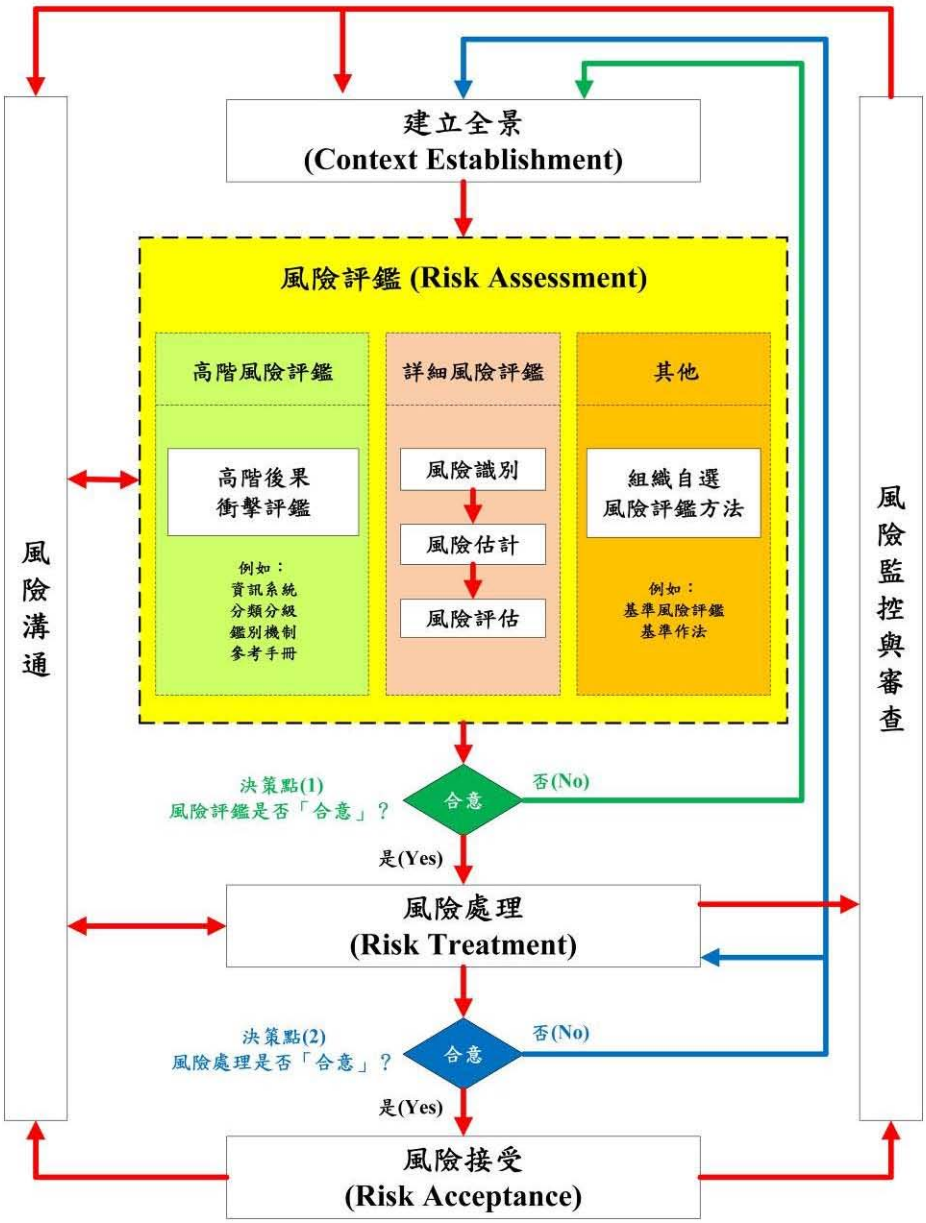
- 風險處理決策點

此決策點讓組織可以依據其所選擇之風險處理方法所獲得的風險處理結果進行「是否合意」的判斷與決策：

– 如果「合意」則結束「風險處理」階段，直接進入「風險接受」階段。

– 如果「不合意」則可能(*1*)重新進入「建立全景」階段，開始另一個風

險管理循環，或者(2)直接回到「風險處理」階段，重新評估與強化風險處理之安全控制措施來改善風險處理結果，直到「合意」爲止。




資料來源：本計畫自行整理

圖9　*ISO/IEC 27005*　風險評鑑多重循環程序圖

### 2.4.1. 高階風險評鑑作法

#### 2.4.1.1. 作法簡介

根據*ISO/ IEC 27005:2008*【附錄 *E*】舉例說明，所謂「高階風險評鑑作法(*High-Level Risk Assessment*)」乃是組織基於各種人力、預算、時間或資源等理由或限制，首先針對其內部所有資訊系統與資訊資產，進行初步的「高階風險評鑑」找出每個資訊系統在該組織的營運業務價值以及「高階衝擊影響」開始，而不用從資產價值、威脅、脆弱性與後果等系統化的詳細風險評鑑開始。針對被識別爲「重要」及/或【高風險/高衝擊影響】的資訊系統，組織如對其風險評鑑結果不合意，可再運用「詳細風險評鑑作法」對其進行另一個風險評鑑循環；至於在「高階風險評鑑」後，屬於「較不重要」或者【較低風險/較低衝擊影響】的資訊系統，組織則可自行根據其安全要求與風險評鑑目標自行選擇適用的風險評鑑方法或者風險處理方式。

#### 2.4.1.2. 作法特色

「高階風險評鑑作法」特色，說明如下：

- 針對組織之所有資訊系統的風險評鑑工作，在準備投入大量專業、人力、時間與預算資源之前，組織先進行快速而簡單的「高階風險評鑑作法」區隔出屬於【高風險/衝擊】資訊系統，則進一步運用「詳細風險評鑑作法」如果屬於【中、低風險】則可直接使用套用該組織認同之基準風險處理作法將能協助組織迅速地建立一個適用於該組織資安政策的風險管理計畫，並有助於該組織的整體資安規劃與持續維護。
- 藉由「高階風險評鑑作法」組織之資源和預算可被最有效的運用，同 時對於該組織最關鍵且需受到保護的資訊系統將會被優先提出與實作，對於後續各項風險處理與應變作爲行動，也將會更爲成功。

#### 2.4.1.3. 作法注意事項

鑑於所有組織因其業務職掌與組織規模不同，同時其業務與資訊系統複雜度、安全等級與系統間關連程度皆有差異，因此在運用本「高階風險評鑑作法」時，組織必須考量下列注意事項：

- 鑑於初期先透過「高階風險評鑑」進行資訊系統重要性與衝擊影響之分 類分級，如果在此階段將較為關鍵重要的資訊系統分類錯誤而被識別成【中、低風險】不需要執行「詳細風險評鑑」，將導致該資訊系統沒有 受到足夠安全等級的防護，此點需要特別謹慎注意。

無論如何，這些高階風險分類分級錯誤的資訊系統至少還有該組織認同之基準風險處理作法之防護措施的保護，因此，組織可以透過「定期」進行高階風險評鑑，重新檢視是否每個資訊系統需要比基準風險處理作法更高的安全防護措施。

- 雖然透過「高階風險評鑑」將重要性與高風險/高衝擊影響的資訊系統區隔出來後，但是後續依然需要投入專業、人力、時間與預算資源來進行「詳細風險評鑑」，對於資訊編制較大或者資源較為充裕的機關而言，資源投入可能問題不大，但是如果要廣泛應用到我國各級政府機關，則需衡量不同規模政府機關，其資源之可用性與可行性，能否勝任「詳細風險評鑑」的工作負擔與落實成效。

### 2.4.2. 詳細風險評鑑作法

#### 2.4.2.1. 作法簡介

所謂「詳細風險評鑑作法(*Detailed Risk Assessment Approach*)」乃是組織針對其內部所有資訊系統與資訊資產，逐一詳查風險，包含深入的識別資產和價值、對資產威脅及脆弱性的評鑑，據以分析風險所造成的機密性、完整性、可用性衝擊與其可能性，然後針對這些分析結果，評估與識別符合該組織

安全等級的防護控制措施。

「詳細風險評鑑作法」主要分成「風險分析(*Risk Analysis*)」及「風險評估(*Risk Evaluation*)」兩項主要活動，其中「風險分析」則可在細分爲「風險識別(*Risk Identification*)」及「風險估計(*Risk Estimation*)」兩項步驟，詳見圖 10 所示，茲分別簡述如下：


資料來源：本計畫自行整理

圖10　詳細風險評鑑作法活動程序圖

- 風險分析 (*Risk Analysis*)

「風險分析」目的是要透過系統化的方式，找出資訊資產的風險，並用「半

定性定量 方式,得出所有資訊資產風險的相對重要性。執行風險分析時，需參考「建立全景階段」所訂定的「風險評估準則」分別識別資訊資產、 威脅發生的可能性、脆弱性被利用的難易度、現有控制措施及威脅與脆弱 性結合發生事故對組織衝擊的後果，以瞭解資訊資產所處環境的資安狀 況。再依據「建立全景階段」所訂定的「衝擊準則」將識別後果的嚴重 性予以分級並量化，藉由評鑑資訊資產的價值、評鑑後果對組織衝擊的嚴 重性及評鑑事故發生的可能性來估算風險值。以資訊安全的「機密性」「完 整性」「可用性」來鑑別資產的價值,即以事故發生時,在「機密性」「完 整性」「可用性」造成的後果，對組織衝擊的嚴重性高低訂定資產價值。 最後將威脅發生的可能性及資訊資產之脆弱性被利用的難易度與資產價 值組合，計算出所有該資訊資產之風險值。

- 風險評估 (*Risk Evaluation*)

風險評估主要是將「風險分析」的結果分等級，再依據「建立全景階段」所訂定的「風險接受準則」以決定需要管控的資訊資產。首先找出所有資訊資產的最大與最小風險值,以計算最大及最小風險值之區間,將之分爲適當等級，例如：普、中、高三個等級；組織再依據其所訂定的「風險接受準則」決定「可接受風險等級」在比「可接受風險等級」值高的所有資訊資產即是需要進一步處理的清單,此資訊資產清單爲「風險處理階段」的對象。

### 2.4.2.2. 作法特色

「詳細風險評鑑作法」特色，說明如下：

- 所有資訊系統之資訊資產均能識別出對該資訊資產適當的防護控制措施。

- 針對每個資訊系統之資訊資產所作詳細風險評鑑之結果,未來可被用在

該組織或者該資訊系統之安全變更的異動管理時參考運用。

#### 2.4.2.3. 作法注意事項

鑑於所有組織因其業務職掌與組織規模不同，同時其業務與資訊系統複雜 度、安全等級與系統間關連程度皆有差異，因此在運用本「詳細風險評鑑 作法」時候，組織必須考量下列注意事項：

- 對於組織內部所有資訊系統之資訊資產，如果皆以詳細風險評鑑進行，將會耗費大量專業人力、時間與預算資源，方能完成所有資訊系統風險評鑑工作，因此組織必須自我衡量資源的可行性與可用性；另外因爲需要評估分析所有資訊系統之資訊資產，可能會因而延宕該組織之真正關鍵資訊系統之安全評估時機。
- 同時詳細風險評鑑作法，將會產生大量的風險分析資料，如果對所有資訊系統之資訊資產，皆以詳細風險評鑑作法進行，可能造成該組織資料維護的負擔。

### 2.4.3. 指引建議架構

本指引運用 *ISO/IEC 27005:2008* 、我國風險管理架構以及「鑑別機制」作爲理論基礎，同時考量我國政府目前資安推廣現況，提出一個適合我國政府的資訊系統風險評鑑架構。