機關需要做風險評鑑嗎？

◎ 鍾榮翰

緒　論

行政院國家資通安全會報為強化各級政府機關資訊安全責任，特於 98 年 6 月 1 日修頒「政府機關(構)資訊安全責任等級分級作業施行計畫」，律訂各級機關依其資安等級應執行之工作項目，其中 A、B 等級機關應於指定期限前通過第三方資訊安全管理系統(Information Security Management System, ISMS)的驗證，C 級機關則應自行成立推動小組規劃作業，驗證範圍應涵蓋機關核心業務資訊系統，並逐步擴大至全機關。本文擬由資訊安全管理之觀點，說明機關為何需要做風險評鑑，及如何選定適用之風險評鑑方法和如何進行風險評鑑作業，以供各級政府機關(構)參考。

壹、風險之定義

依據 CNS 14929-1 資訊技術－資訊技術安全管理指導綱要第 1 部顯示：資訊技術安全概念與模型，提供了一個「安全元件關係模型」，有助於我們了解資訊安全之風險，詳如圖 1 所示。

風險的定義：已知威脅利用單一或一群資產的脆弱性，造成資產損失或損壞的潛在可能性。

依據以上之定義，由圖 1 安全元件關係圖中可以看出，一旦已知威脅(T)利用了資產存在的脆弱性(V)(或稱之為：弱點)，存在著不同程度的發生機率，會對資產造成不同程度之衝擊，綜合之後的結果便是風險(R)；換言之，一個事故的發生可能機率很高，但是衝擊的程度卻很小，也有可能是發生的機率非常低，但卻會造成極其嚴重的衝擊。

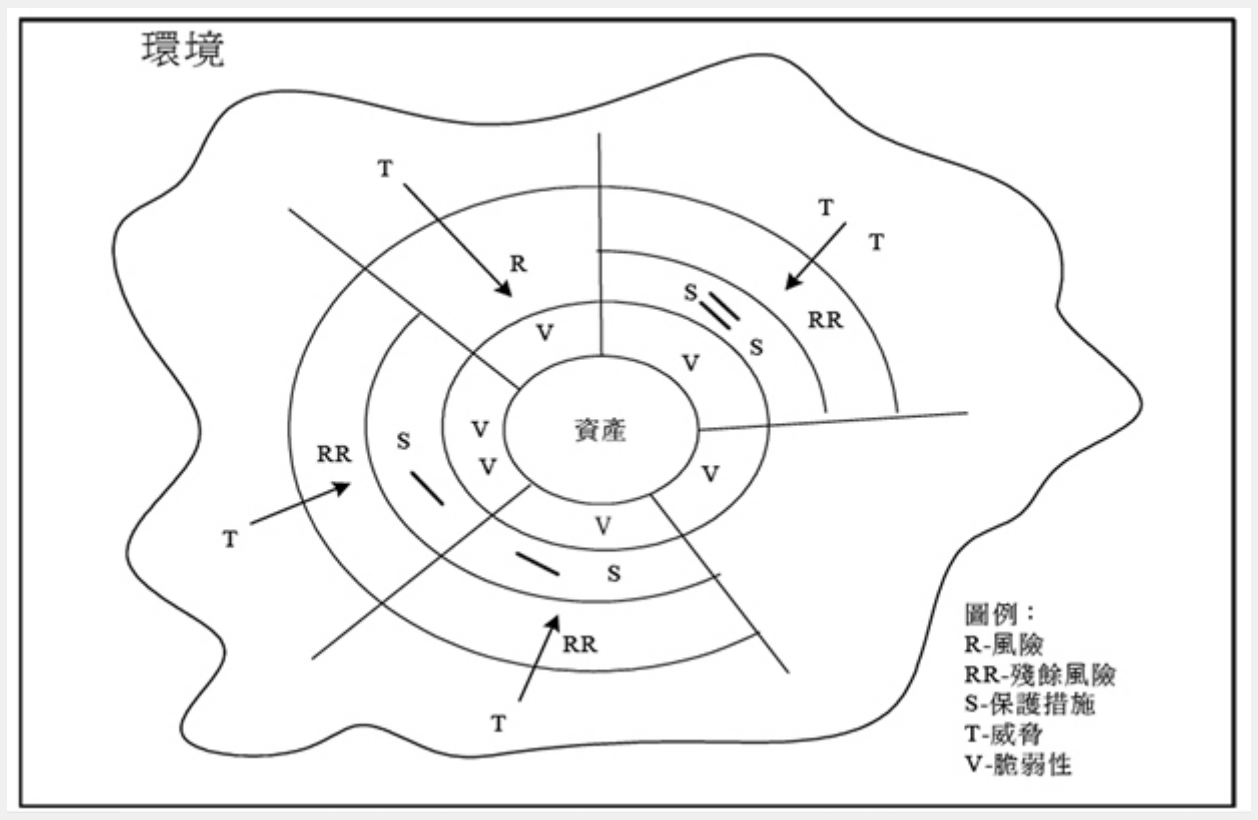

圖 1 安全元件的關係圖

要進行風險評鑑，便要找出機關所擁有的「資產」，分析「已知的威脅」，如何利用資產的「脆弱性」，評估其發生「機率」與「衝擊」之程度，若綜合之後的結果是機關所無法接受者，便要進行風險處理，運用保護措施(S)讓殘餘風險(RR)降低至機關可接受之水準。

以上是由資產的觀點，來解釋風險。接下來將從風險管理的角度來說明各種安全元件之關係。資產的定義係指對組織有價值的任何事物，所以資產的價值越高，對組織營運的衝擊也會越大，相對地風險便會提高；若資產之脆弱性被曝露，導致被威脅利用，都會使風險增加。依據風險之高低，決定防護之需求，而防護措施必須滿足防護的需求，藉以防止威脅利用脆弱性，如此才可達到降低風險之目的。

根據以上的說明，行政院爲改善所屬各機關治理、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，所以機關識別其各項安全要求，絕對是必要的，而風險評鑑便是主要的途徑之一。

貳、風險評鑑的窒礙

根據以上的安全模型，我們可以很容易地了解風險評鑑的重要性，以及各安全元件之關係。但是實際要執行風險評鑑的過程，卻常遭遇以下的窒礙因素，而導致未能鑑別出機關所面臨之風險，因而造成資安事故的不斷發生。

一、資產的識別

從安全的觀點而言，如果沒有識別組織的資產，就不可能實作和維護成功的安全計畫。實務中以下的資產，很容易被列爲清查的對象：

1. ●資訊：資料庫及資料檔案、系統文件、使用者手冊、訓練教材、作業及支援程序、業務永續運作計畫、備援作業計畫等。
2. ●軟體：應用軟體、系統軟體、開發工具及公用程序等。
3. ●實體資產：電腦及通訊設備、磁性媒體資料及其他技術設備。
4. ●技術服務：電腦及通信服務、其他技術性服務(如電源及空調)。
5. 人員：人員資格、技能及經驗。

但是依據國際資安風險管理標準 ISO/IEC 27005:2008 Information technology — Security techniques — Information security risk management 附錄 B[6]，則建議將機關業務程序與活動，及活動所產生之資訊列爲主要資產，將硬體、軟體網路、人員、場所及組織架構等視爲支援性資產，著重點於機關之施政業務活動。

另一個執行的窒礙在於資產鮮少單獨存在，從安全元件關係圖中，無法看出資產與資產之關連性。以機關處理公文爲例，若一份公文中有三份附件，其機密等級分別爲普通、密、機密，則當三份附件同時附加於同一份公文中，則此公文之機密等級將會套用最高原則，應判定爲「機密」；反之，若本文與附件分置，則本文之機密等級也將取消。以上之觀念對公務人員而言，應是基本的公文處理保密概念，但是在資訊安全風險評鑑實務中，卻鮮少被提出並實作，而導致費時費力，卻未能有效地降低風險。

二、威脅之識別

依據風險之定義著重點於「已知的威脅」，亦即已知的威脅才有辦法加以降低：反之，若是「未知的威脅」，則無法加以防範，其對象包括新興的威脅，或是未被機關識別出的威脅。至於威脅如何利用脆弱性之情境，包含事故可能發生之人、事、時、地、物、如何、爲何等，都應加以描述並予詳盡的評鑑程序。

三、分析的方法

風險分析的深入程度會隨著所獲得的資訊與數據而有所不同。一般而言，風險分析包括定性分析、半定量分析、定量分析，及綜合上述三種方法的分析。分析的複雜度及所需的費用，由低至高分別是定性分析、半定量分析、定量分析。通常一開始會使用定性分析，先大致了解風險的等級，之後再依需求決定是否使用更精確的定量分析。詳細說明請參閱行政院風險管理及危機處理作業手冊。

參、風險分析的方法

風險分析策略應確保所選擇之作法適合於該環境，且盡全力將安全聚焦在真正需要之處。以下說明三種不同的風險分析作法，每一選項間之基本差別在於風險分析的深度。由於對 IT (Information Technology)系統做詳細的風險分析，成本往往過高，而對嚴重風險只給予極少的重視亦不具效益，故需要在諸選項之間考量風險與成本的平衡。詳如圖 2 所示。摘要說明如下：

一、基準作法(Baseline Approach)

不需對組織內風險不高的資產逐一清查風險，直接引用國內外標準或指引，選擇所需的基準安全(Baseline)。可藉由選擇防護措施而將基準安全應用到所有的 IT 系統。

(一) 選擇基準作法的特色

1. ●只需要最少量的資源做風險分析及管理每一防護措施實作，因而可減少時間和花費在選擇防護措施的工作量。
2. ●若某組織的多數系統係在一共同的環境下運作且安全需求相近，由於相同或類似的基準防護措施無需太大的工作量便可被許多系統採用，故基準防護措施爲具成本效益的解決方案。

(二) 選擇基準作法應注意事項

1. ●如果基準等級設得太高，在某些 IT 系統上的安全等級可能會超過太多，造成資源的浪費。
2. ●如果基準等級設得太低，在某些 IT 系統上可能會有安全的不足，而造成高度曝露於風險中。
3. ●在管理與安全攸關的變更時可能會有困難，例如：若將某系統升級，可能難以評鑑原始基準防護措施是否仍充足。

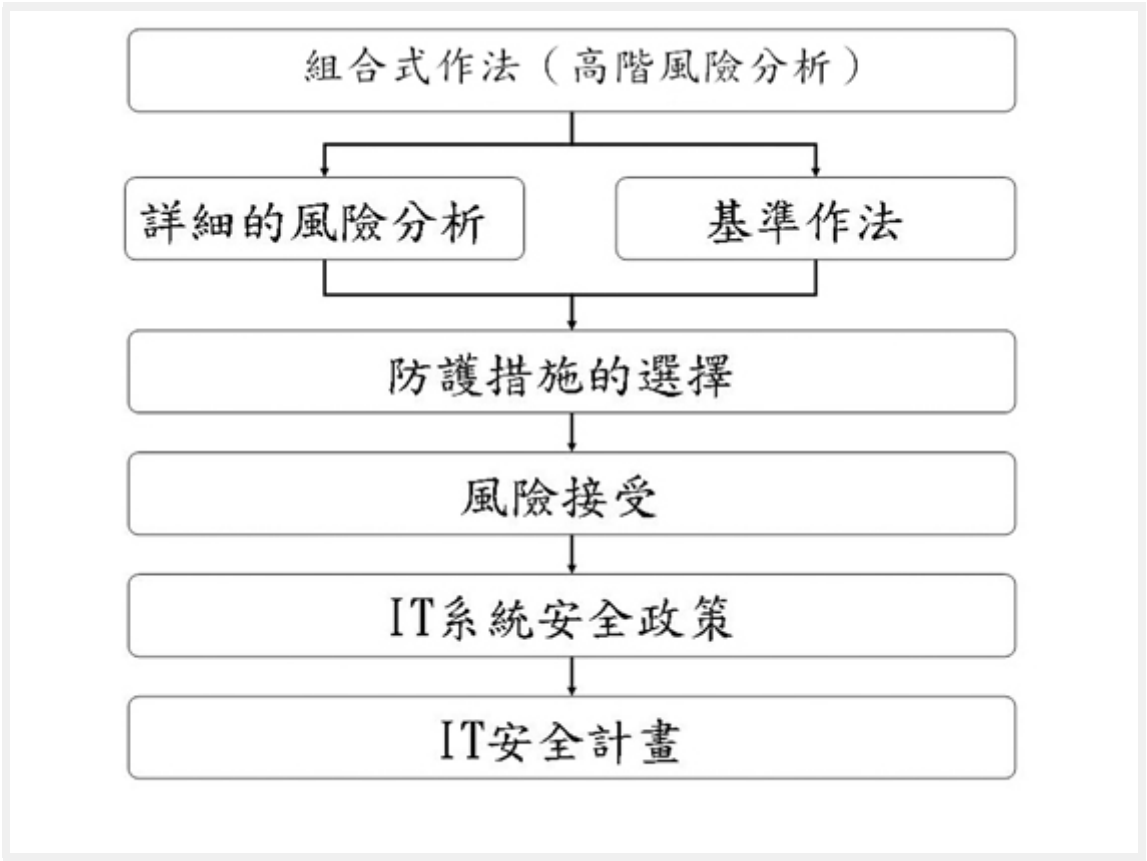

圖 2 風險評鑑流程圖

(三) 建議

若某組織的所有 IT 系統只有低等級的安全需求，則此作法可能是最具成本效益的策略。多數組織將需要符合某些最低的標準以保護敏感資料並遵循法律與條例(例如：個人資料保護法)。在此個案中，必須選擇反映大多數 IT 系統所要求之保護程度的基準。無論如何，若組織內各系統的營運敏感性、規模與複雜度均不同，想以一套共同標準應用到所有系統，是既不合邏輯又不具成本效益。

二、詳細的風險分析(Detailed Risk Analysis)

詳細的風險分析包含深入的識別資產和估價、威脅對資產的評鑑，及脆弱性的評鑑，據以分析風險所造成的衝擊與其可能性。從這些活動所得的結果將使用在評鑑風險，然後用以識別正確的安全防護措施。

（一）選擇詳細的風險分析作法的特色

1. 所有系統均能識別出對該系統適當的防護措施。
2. 詳細的風險分析所得結果可被用在安全變更的管理。

（二） 選擇詳細的風險分析作法應注意事項

1. ●由於所有 IT 系統會以相同的方式詳細考量，這需要大量的時間去完成分析，關鍵系統之安全需要被提出時可能爲時已晚。
2. ●此作法將產生大量的分析資料，若對所有 IT 系統要求以相同的方式詳細考量，將造成資料維護的負擔，也容易發生相同風險卻有不一致的評價結果。

（三）建議

此作法需要大量的時間去完成分析，不適合對所有 IT 系統執行詳細的風險分析，可以局部用於重要性較高的 IT 系統。

三、 組合式作法(Combined Approach)

首先對所有的 IT 系統作初步的高階風險分析(High Level Risk Analysis)，在每一個案中，集中在 IT 系統的營運價值以及它被曝露在那些嚴重風險處。至於被識別爲對組織營運重要及／或被曝露在高風險處的 IT 系統，宜優先進行詳細的風險分析。對所有其他 IT 系統，則選擇基準作法。這種組合式作法，能在識別防護措施花費的時間和工作量降至最低之間，提供一個良好的平衡，且能確保各高風險系統都受到適當的保護。

(一) 選擇組合式作法的特色

1. ●在投入大量時間與資源之前，先進行初期迅速而簡單的風險分析作法(高階風險分析)，可得到一種廣被接受的風險分析計畫。
2. ●能迅速建立一個組織安全計畫的策略構圖，此策略構圖將成爲良好的輔助規畫。
3. ●資源和金錢可被最有效的運用，最需要受到保護的系統將會被優先提出，且後續各項作爲行動將會更爲成功。

(二) 選擇組合式作法應注意事項

如果初期的風險分析是在高階，其結果可能較不精確，某些較重要的系統有可能被識別成不需要執行詳細的風險分析。但無論如何，這些系統仍將受到基準安全的保護，而且這些系統可在必要時被重新訪查，以檢查是否需要比基準作法更多的防護措施。

(三) 建議

先使用高階風險分析，再組合上基準作法及詳細風險分析，是平衡風險與資源兩者最適合的作法，此爲大多數組織最有效的作業方法。

肆、結論

自行政院國家資通安全會報大力推動 ISMS 驗證以來，各級機關大多採用 ISO/IEC 27001 之標準。該標準適用於一般型之組織，將每一個機關都視爲單一的組織，所以多建議採行詳細風險分析作業，並未考量經濟規模；若遵循之機關數量眾多，站在主管機關之立場，下轄機關中不乏組織結構相當、業務性質雷同者，何以不能依據其防護需求，律訂低中高不同之防護等級，供各級機關遵循以講求成本效益？各國政府成功之案例，多採行基準法或組合式作法。行政院研考會亦積極規劃適用於我國政府機關之專屬資安認驗證體系，改採依據資訊及資訊系統分類鑑別機制，遵行組合式風險評鑑作法，擷取各式分析方法之優點，以落實資訊安全管理爲目的，明確、有效、易於遵循爲原則，提供各級機關遵循。

（作者爲國家資通安全會報技術服務中心經理）