國際資訊安全標準 ISO 27001 之網路架構設計 －以國網中心為例探討風險管理

李慧蘭
國家實驗研究院國家高速網路與計算中心
gracelee@nchc.org.tw

摘要

ISO 27001:2005 是資訊安全的國際標準。該標準協助組織降低資訊脆弱點所造成的損失及預防潛在風險的衝擊。傳統建構資訊安全的元素不外乎由防火牆、IDS、IDP 等等所組成，缺乏一套系統性的分析工具，ISO27001 標準的作業程序是將資訊資產列表，依據這些資產本身所存在的弱點，預測會面臨的威脅，進而評估該風險是否為組織可承受。國家高速網路與計算中心致力於建置高品質學術研究之平台，透過高速網路提供高效能計算主機、高容量儲存設施與主機代管服務。本文將以 ISO27001 的標準規範為基礎，介紹本中心在取得 ISO27001 認證的過程中，如何作風險評鑑，針對高風險資產規劃控制措施作風險處理，以設計出符合本中心風險期望之網路架構。

關鍵詞：ISO27001、ISMS、風險評鑑、風險處理、資訊安全。

Abstract

ISO 27001 is a new standard demonstrates a systematic approach to establish a system (ISMS) to guarantee the information security. The ISMS is established based on clever risk assessment to figure out high risk vulnerable assets and risk treatment to reduce the risk level below an acceptable level. National Center for High-Performance Computing recently applied this standard for the high performance storage system, and network is within the scope. In this paper, we introduce this standard briefly, describe the definitions in risk assessment, and contribute our experience establishing ISMS. Finally, we conclude a secure network architecture design to fit our organization's risk expectation.

Keywords: ISO 27001、ISMS、risk assessment、risk treatment、information security.

1. 前言

目前的網路安全設備技術效能日新月異，儘管如此，資訊安全事件仍是層出不窮，其基本的原因在於”人”的疏忽，就如沒有良好的交通規則、號令，性能再好的車子在路上也是動彈不得。同樣的道理，如果沒有良好的作業準則，效能再好的網路安全設施，依然無法杜絕層出不窮的資安事件，更提不上防微杜漸了。

因此我們必須重新檢視資訊安全的定義。從會計的角度，將我們生活周遭的資訊分門別類定義為一個一個不同的資產類別。根據每個資產類別去定義資產價值和風險評估。由資產價值和風險評估決定出該資產的風險等級。針對高風險資產，制定出風險處理計劃書，以採取行動降低該資產的風險。

而 ISO27001 的核心就是建立 ISMS，以提供一個資訊安全作業準則的平台，藉由這個平台，各個單位可以透過完整而綿密的資訊資產風險評估，建立一套量身訂作風險降低政策以降低資產的風險，透過管理層面的完善規範，可以確保資安事件的發生在可以容忍的風險程度內。

在本文中，侷限於有限的篇幅無法完整介紹 ISO 27001，因此，我們先對 ISO 27001 作一簡短的介紹，再將注意力集中在 ISO 27001 ISMS 的建立過程中最重要的風險評鑑和風險處理步驟。風險評鑑就是整理出所有資產清單，並列出資產面臨的弱點和威脅，接著計算資產*總風險值*。風險處理就是針對高總風險*值*的資產作出風險處理計劃書，以降低該資產風險等級至可以接受的程度。

最後再以國家高速網路與計算中心(以下簡稱國網中心)為例說明如何作資產的風險評鑑，針對高風險資產，擬定風險處理計劃書，其中會擬定資訊風險降低對策，再配合風險降低對策建置一個符合組織需求低風險的資訊系統。

2. ISO 27001 標準

ISO27001 的前身是 BS7799，BS7799 是英國的資訊安全國家標準，其中 BS7799 part2 的部份於 2005 年演變為資訊安全國際標準，即 ISO27001:2005[2][3][6]。ISO27001:2005 的內容主要定義了驗證的規範。根據 ISO 27001 的精神，驗證的範圍可由組織視需要自行決定。

ISO 27001 的結構如圖 1 所示，整個標準的重心都是放在 ISMS 上面，而第四章，特別說明如何發展組織的 ISMS。章節和章節間形成一個 PDCA 框架如圖 2 所示，PDCA 是 Plan-Do-Check-Act 的縮寫。代表程序需要被規劃(Plan); 實作、操作和維護(Do); 監控、稽核和重新檢討(Check)以及改進(Act)。

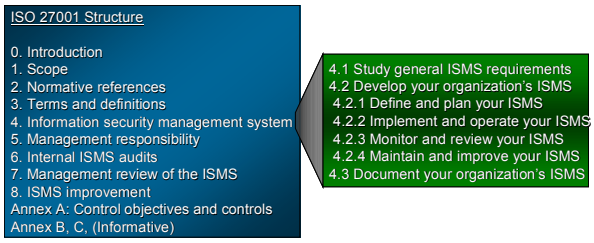


圖 1 ISO 27001 的結構

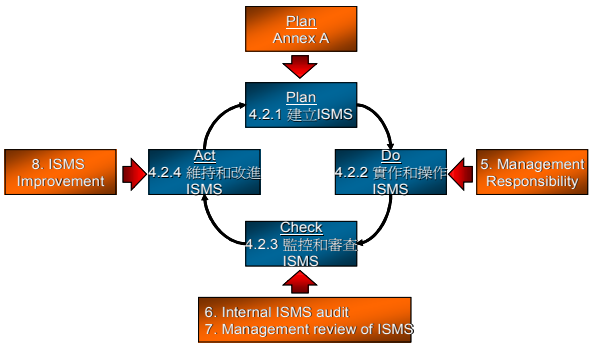


圖 2 ISMS Framework

資訊安全的確保必須透過一套合宜的管理(包含: 政策、步驟、程序、組織架構以及軟硬體的功能)才可以實現。這也是，為什麼 ISO 27001 的重心就是去建立一個 ISMS 的資訊安全管理系統。

3. ISMS 資訊安全管理系統

所謂 ISMS (Information Security Management System) 就是一套基於系統性商業風險評估方法的管理系統以建造、執行、運作、監控、檢閱、維持以及改進資訊安全。它是一套有組織的方法以確保資訊安全。

ISMS 的建立程序可以分為 10 個要點(4.2.1.a ~4.2.1.j)，可以用下圖來說明，其中 4.2.1.c、4.2.1.d 和 4.2.1.e 歸屬於風險評鑑。而 4.2.1.f、4.2.1.g 和 4.2.1.h 歸屬於風險處理。

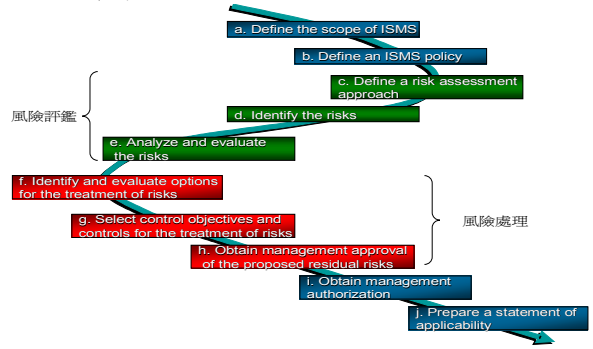


圖 3 ISMS 建置流程

ISO27001 的精神是希望組織由上到下均能貫徹合乎組織目的之資訊安全系統。先是由管理階層根據組織業務的需求訂定資訊安全範圍和資訊安全政策。緊接著，即是在資訊安全系統範圍內的單位，對資產進行風險評鑑，針對高風險資產參照附錄 A 的控制目標和控制措施進行風險處理，在取得管理階層的授權後，擬訂適用性說明書，便可依序進入 PDCA 模型的 Do、Check 和 Act 階段，見圖 2。

一個完善的 ISMS 系統的建立根植於風險評鑑和風險處理。因此，我們在這篇文章的討論重心放在建立 ISMS 中的風險評鑑和風險處理上，同時輔以國網中心的實際案例作為說明。

4. 風險管理

一個可以信賴的組織會評估它定義的資產，決定出那些風險是它無法容忍並針對無法容忍的風險去作好控管，以謹慎考量的政策或流程去管理殘餘風險。是為風險管理。

風險管理可以分成兩個部份，第一部份，就是風險評鑑，根據資訊安全管理系統範圍內的資產，評鑑其風險等級。第二部份，就是針對高風險資產作風險處理，降低其風險，使其一旦發生風險時，仍然在可以接受的範圍內。

4.1 風險評鑑

風險評鑑的第一個步驟，就是先定義風險評鑑的方法。在 4.1.1 節將說明，國網中心如何去定義量化的風險評鑑方法以及定義風險等級。接著即是要盤點在資訊安全管理系統範圍內的資產盤點。根據每項資產思考可能會存在的脆弱點，根據可能會發生的威脅，思考該項資產的脆弱點，以及該威脅發生時對組織的影響程度。依照 4.1.1 節的量化方法，計算出一個總風險值。得到總風險值後，我們便可以依據 4.1.2 節所定義的風險等級表，去換算出其對應的風險等級。

4.1.1風險計算

簡而言之，風險計算就是算出該資產的總風險值，而總風險值，可由下列式子[1]得到一個數值

總風險值 = 資產價值 × 破壞事件嚴重程度

其中，資產價值和破壞事件嚴重程度分別於後面兩個小節簡介。

4.1.1.1資產價值

所謂資產價值的評價，就是分別針對機密性評價、完整性評價和可用性評價，加總以求得其總體的資訊資產價值。如以下式子[1]表示:

資產價值 = 機密性評價 + 完整性評價 + 可用性評價

機密性、可用性和完整性的評價可以根據標的資產有不同的定義，但是基本的精神是相同的，以下，我們將就設備資產價值定義為例。

表 1 機密性，完整性，可用性評價參照[1]

評價	機密性	完整性	可用性
1	不限制使用之資訊處理設施與系統資源等。	不當的破壞或竄改資訊、資訊處理設施與系統資源，所造成的業務衝擊可以忽略者。	工作日之上班時間至少 25%的時間有權限的人可存取資訊系統與資源。
2	非公開使用之	不當的損失、破壞	工作日之上班時間

	非敏感性資訊處理設施與系統資源為者。	資訊處理設施與系統資源，會對業務應用造成輕微的衝擊。	至少 50%的時間有權限的人可存取資訊系統與資源。
3	敏感性資訊處理設施與系統資源，僅開放給必要知道的人使用。	不當的損失、破壞資訊處理設施與系統資源，會對業務應用造成顯著的衝擊。	工作日之上班時間有權限的人都可存取資訊系統與資源。
4	敏感性之資訊處理設施與系統資源，僅開放給極少數必要知道的人使用。	不當的損失、破壞資訊處理設施與系統資源，會對業務應用造成很大的衝擊，甚至會造成業務失敗。	工作日(24 小時)，至少 95%的時間有權限的人可存取資訊系統與資源者。

4.1.1.2 破壞事件的嚴重程度

要評價破壞事件的嚴重程度，我們就必須要分別對該資產去考量可能的威脅等級評價(系統被攻擊的頻率)，見表 2[1]，面對威脅該資產的脆弱點等級評價(系統被攻擊的容易度)，見表 3[1]，和該威脅發生時對組織所造成的衝擊等級評價(系統被攻擊所造成的影響程度)，見表 4[1] 。同時定義破壞事件嚴重程度如下公式[1]:

破壞事件的嚴重程度 = 威脅等級 × 脆弱點等級 × 衝擊等級

表 2 威脅等級評價表

威脅等級評價	說明
1	威脅來源缺乏動機而且能力不足
	防制脆弱性被利用的安全對策有效
	不太可能發生 (沒有發生過，但是有發生的可能)
2	威脅來源缺乏動機且能力不足
	防制脆弱性被利用的安全對策有效
	發生頻率低 (平均每年發生的次數不到一次)
3	威脅來源有動機也有能力
	防制脆弱性被利用的安全對策有效
	有可能發生 (平均每年都可能發生一次以上)
4	威脅來源有強烈的動機與足夠的能力
	防制脆弱性被利用的安全對策無效
	時常發生 (平均每月都可能發生一次以上)
5	威脅來源有強烈的動機與足夠的能力
	防制脆弱性被利用的安全對策無效
	發生頻率非常高 (平均每週都可能發生一次以上)

表 3 脆弱點等級評價表

脆弱點等級評價	說明
1 (低) 很難被利用	1.必需運用特殊的方法才能利用脆弱點進行攻擊
	2.威脅來源必須花費長時間(可能需一個月以上)的資料收集,突破各層防護,才能接觸到關鍵資訊
	3.攻擊成功:可能要 1~數個月
2 (中) 被利用難度適中	1.不需用特殊的方法就能利用脆弱點進行攻擊;
	2.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)進行資料收集即能接觸到關鍵資訊
	3.攻擊成功:可能是數天以上
3 (高) 很容易被利用	1.利用簡易的方法就能利用脆弱點進行攻擊
	2.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
	3.攻擊成功:可能是一天內到數天

表 4 衝擊等級評價表

衝擊等級評價	說明
0 (可忽略)	1.對於業務執行沒有影響; 2.可以立即完成復原
1 (微弱)	1.對於業務執行沒有影響; 2.可以立即完成復原 3.若持續發生且次數頻繁,對業務執行可能帶來潛在風險
2 (輕微)	1.對於公司整體業務執行影響不大; 2.造成的損失可能僅影響單一業務或系統; 3.損失可能影響僅個人或少數幾人; 4.可以由個人進行復原; 5.修復或進行復原的措施可以在很短時間(1 小時)內完成
3 (嚴重)	1.對於公司整體業務執行造成損害; 2.造成的損失可能影響多種業務或數個系統; 3.損失可能影響多個部門或合作夥伴; 4.復原的措施必須由專業人員才能進行;
	5.復原可能要數個小時~到一天才能完成
4 (癱瘓)	1.公司整體業務執行造成損害; 2.事件處理不當可能對公司形象造成損害; 3.造成的損害可能影響全公司; 4.系統或相關服務停頓或癱瘓,業務無法運作; 5.合作夥伴或客戶失去信心; 6.復原的措施僅能由特定專業人員才能進行或修復人員不易取得; 7.復原無法於一天才能完成; 8.可能造成人員傷亡

4.1.2訂定風險等級

將總風險值的最大值和最小值相減再分成四個等分，即可得到風險等級的級距，以國網中心為例，最高的總風險值為 720，最低的總風險值為 0，因此，即可得到如下的國網中心的風險等級表。

表 5 風險等級表

風險等級	起始值	結束值
A	540	720
B	360	539
C	180	359
D	0	179

在國網中心專業資訊安全管理委員會的決議，即訂定，可接受的風險等級為 D，亦即，風險等級為 C 以上者，就必須作風險處理以減輕其風險。

4.2 風險處理

經過前面的步驟，作好資訊安全管理系統範圍內的資產盤點和風險等級評鑑後，可以得到資產的風險等級分佈，針對高風險等級的資產作風險處理。風險處理計劃通常包含了 4 個目的

1. 消除風險
2. 將無法消除的風險，透過控制機制將其降低到可以接受的程度
3. 如果決定和風險共存，就必須透過謹慎的控制讓風險的發生仍維持在可以接受的範圍。
4. 或者，用另一種思維，透過保險或簽定維護合約的方式將風險轉移到其他的協力廠商。

4.2.1評估殘餘風險

但是在加入控制措施後，我們還必須考慮，加入的控制措施是否能夠移除威脅發生的可能，降低威脅所發生的頻率或是降低威脅所造成的衝擊，再依前面風險評鑑的方法，重新作威脅等級評價，脆弱點評價及衝擊等級評價。再去檢視其殘餘風險等級是否在可以接受的風險程度內。如果，還是高於可接受風險等級，就可以增加控制目標以及對應的控制措施，以降低其風險等級。

若增加控制目標無法將風險降到可以接受的等級，或是增加控制措施的成本太高時，可以考慮透過保險，將風險轉嫁給保險公司或是維護合約，將風險轉嫁給協力廠商。

5. 國網中心網路風險管理

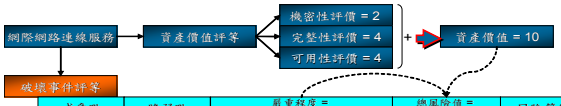
國網中心針對高效能儲存系統作 ISO 27001 認證，我們將就此經驗作一分享。網路也在這個認證範圍內，因此，在文中針對國網中心的網路相關資產作風險管理作業。就實體設備而言，不言可喻它所遭受到最大的威脅，就是會遭到人為的破壞

或電源不穩定，而造成服務中斷的嚴重衝擊。但是國網中心有集中而且嚴格的門禁管制機房和充足功率的備援發電系統，因此，這兩種威脅便可以移除。使得實體設備的風險等級均於可以接受的風險等級內。

受限於篇幅的關係，我們僅就網際網路連線服務、伺服器服務這兩項服務資產作風險管理介紹。

5.1 網際網路連線服務風險管理

網際網路連線服務該項資產是由一個群組的資產: 包含路由器、對外線路連線、路由協定等以提供的網際網路服務。這個服務最主要的工作，就是提供國網中心可連線至網際網路。針對這個服務資產所作的風險評鑑如圖 4。



威脅點	脆弱點	嚴重程度 = 威脅等級 * 脆弱等級 * 衝擊等級	總風險值 = 資產價值 * 嚴重程度	風險等級
中斷	IOS更新	3 * 3 * 3 = 27	10 * 27 = 270	C
	維護不當	4 * 2 * 2 = 16	10 * 16 = 160	D
	對外連線中斷	2 * 2 * 3 = 12	10 * 12 = 120	D
	內部線路中斷	2 * 1 * 3 = 6	10 * 6 = 60	D
	router chassis故障	1 * 1 * 4 = 4	10 * 4 = 40	D
	模組故障	2 * 2 * 4 = 16	10 * 16 = 160	D
	火災	1 * 1 * 4 = 4	10 * 4 = 40	D
	停電	3 * 1 * 4 = 12	10 * 12 = 120	D

圖 4 網際網路連線服務風險評鑑

5.1.1網際網路連線服務資產價值

首先我們必須對這項資產作一資產價值評等。所以參照表 1 的機密性，完整性和可用性來作評價。茲整理如下:

- 機密性: 這項服務，允許網際網路上的所有使用者使用中心的服務，但是，在中心內部網路，只允許內部員工使用這項服務，外來訪客必須透過申請才能使用這項服務，因此評價是 2。
- 完整性: 如果，不當的損失會對業務造成很大的衝擊，因此評價是 4。
- 可用性:最適合這項的資產的描述是，工作日(24 小時)，至少 95%的時間，有權限的人可以存取這項資產，因此，評價是 4。

依據 4.1.1.1 的定義，資產價值就是三個評價的加總，亦即是 10。

5.1.2網際網路連線服務破壞事件嚴重程度

再計算好資產價值後，我們要作的工作，就是去思考這項資產的可能威脅點，及以對應這個威脅的脆弱點，評估這個威脅所造成的衝擊程度。根據這些資料來評估威脅所可能造成的嚴重程度。

舉例來說，如圖 4，網際網路連線服務潛藏的中斷脆弱點可能會造成服務中斷的威脅。造成服務中斷的脆弱點，有可能是因為 router IOS 更新、管理人員維護不當、對外連線電路中斷、內部線路中斷、router chassis 故障、模組故障，火災或是停電。

這些原因整理好後，我們要分別針對威脅點、脆弱點和衝擊程度依表 2、表 3 及表 4 去作評價。然後將分別所得到的評價相乘以計算其嚴重程度。

首先，檢視 router IOS 更新後必須重新開機所造成的中斷。之所以要作 IOS 更新，就經驗而言，IOS 常常會有我們不知的 bug，而且，有些新的功能是舊版 IOS 所無法提供，舉例來說，目前我們的 IOS，並不支援 BGP IPv6 multicast address family，但是，IPv6 multicast 又是國網中心要推展的業務，所以當有符合我們需求的 IOS 推出後，就必須要作 IOS 的更新。

因 IOS 更新所造成的服務中斷，其威脅評價，脆弱點評價和衝擊點評價整理如下:

- 威脅評價: 就頻率來說，平均每年都有一次以上，依表 2 的定義，評價等級是 3。
- 脆弱點評價: 一旦發現所需的服務不支援或是有 bug，就必須更新，很容易需要更新 IOS，依表 3 的定義，評價等級是 3。
- 衝擊點評價: 因為更新所造成的中斷，會影響到中心的業務，而且會影響到多個業務或是數個系統，依表 4 的定義，評價等級是 3。

最後，我們可以得到 IOS 更新所造成的中斷的嚴重程度為三者的相乘，即得到 27。

依此類推，即可得到其他中斷-脆弱點的嚴重程度，如圖 4 所示。

5.1.3網際網路連線服務風險等級

我們必須透到 5.1.1 所得到的資產總值，和 5.1.2 所得到的嚴重程度，兩個值的乘積即定義為總風險值，透過風險等級表(表 5)的轉換,即可得到該資產面對該威脅和脆弱點的風險等級。

我們再回過頭來檢視 IOS 更新所造成的服務中斷由 5.1.2 所得到的嚴重程度為 27，根據 5.1.1 的資產總值為 10，所以得到風險總值是 270。再透過風險等級表(表 5)的換算，可以得到風險等級為 C。依此類推，我們可以得到其他威脅-脆弱點的的風險等級如圖 4。

因為，我們可以接受的風險等級為 D， 因此，我們必須針對 IOS 更新所造成的中斷作風險處理。

5.1.4網際網路連線服務風險處理

針對 IOS 更新所造成的中斷，我們擬定了 router 備援的控制目標，目的在於當一台 router 在作 IOS 更新時，另一台 router 可以接替第一台 router 繼續工作，不致於使網路造成中斷。以消除 IOS 更新所造成的風險。

控制措施，即是再加購一台 router，補足模組，可以作 1:1 的備援。兩台 router 彼此之間執行 HSRP 協定[5]，讓這兩台 router，邏輯上看起來就如同一台 router，這樣一來，就可以移除 IOS 更新所造成的中斷風險。

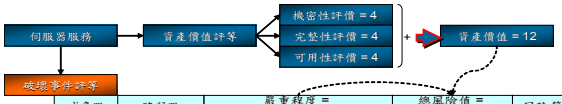
5.1.5網際網路連線服務殘餘風險

透過新增的控制目標和控制措施，就可以消除 IOS 更新所造成服務中斷的風險。

5.2 伺服器服務風險管理

我們知道，伺服器服務這個資產，其實包含很多實體資產在內，如: 磁碟機、備份伺服器、負載平衡伺服器等，但在這裏我們只針對網路相關資產去作評價，因此我們定義伺服器服務這個資產

是由一個群組的資產: 包含伺服器、交換器、路由器等以提供的網際網路伺服器服務。針對這個服務資產所作的資產評鑑如下圖。



威脅點	脆弱點	嚴重程度 = 威脅等級 * 脆弱等級 * 衝擊等級	總風險值 = 資產價值 * 嚴重程度	風險等級
中斷	維護不當	3 * 2 * 2 = 12	12 * 12 = 144	D
	模組故障	2 * 2 * 3 = 12	12 * 12 = 144	D
	火災	1 * 1 * 4 = 4	12 * 4 = 48	D
	停電	3 * 1 * 4 = 12	12 * 12 = 144	D
入侵	維護不當	3 * 3 * 3 = 27	12 * 27 = 324	C
	病毒感染	3 * 3 * 2 = 18	12 * 18 = 216	C
	存取控管	1 * 1 * 4 = 4	12 * 4 = 48	D
	DoS/DDoS	3 * 3 * 2 = 18	12 * 18 = 216	C

圖 5 伺服器服務風險評鑑

5.2.1伺服器服務資產價值

類似 5.1.1 的算法，我們可以得到機密性評價、完整性評價和可用性評價分別都是 4，所以該項服務資產的資產價值為 12。請參照圖 5。

5.2.2伺服器服務破壞事件嚴重程度

在思考可能的威脅點和脆弱點後，我們整理如圖 5。可能造成中斷威脅的脆弱點有維護不當、模組故障、火災、停電。而可能造成入侵威脅的脆弱點有維護不當、病毒感染、存取控管不當以及 DoS/DDoS。

中斷威脅的分析，大致就如同 5.1.2，而詳細的嚴重程度分析如圖 5 所示。在此，我們將集中在於說明入侵威脅的分析。

■ 因維護不當所造成的入侵威脅:

以國網中心的格網服務為例，一開始為了方便維護，格網服務的控管都是由相關單位自行維護，並沒有功能性的區隔。當網路的規模還不大的時候這樣分散式管理，很有效。但是，當網路的規模和提供的服務日益擴大，網路管理人員很容易因為疏忽犯了維護不當的問題。以致於該開放的服務沒開，或是該保護的 port 沒保護到，導致系統被攻擊，造成的巨大衝擊。就頻率而言，很有可能一年發生一次以上，威脅等級評價為 3，而這個脆弱點很容易被利用，因此，脆弱點等級為 3，一旦這個入侵威脅發生後所造成的衝擊程度，依表 4 的定義，評價為 3。嚴重程度即為三者的乘積，即得到 27。

■ 因病毒感染所造成的入侵威脅:

因為作業系統漏洞所造成的病毒感染，而導致被植入後門漏洞的消息，屢見不鮮。誠如上述所言，原先中心的網路都是採用分散式管理，所以，對外服務網路和辦公網路在實體上是連在一起的。而且，隨著網路規模的擴大，頻寬的擴充，目前國網中心的對外頻寬高達 10Gbps，若要佈署 Firewall，只能佈署於對外的專線闡道，因為需要高效能處理能力的 Firewall 成本太高，而且擴充性不佳，所以，在目前，只是透過 router 的 ACL 作基礎的管理。因此，並無法有效的防範病毒由網際網路入侵中心的網路。威脅等級，脆弱點，和衝擊程度的評價，分別是 3、3 和 2。所得到的嚴重程度為 18。

■ 因存取控管不良所造成的入侵威脅:

存取控管不良，造成外來者得以入侵機房或管線，從中入侵到網路中，竊取機密資料，破壞服務完整性，或是破壞服務可用性。但是，因為，國網中心有嚴格的訪客管制，同時，機房亦有門禁的嚴格控管，因此，威脅等級、脆弱點、程衝擊程的評價，分別是 1、1 和 4。所得到的嚴重程度為 4。

■ 因 DoS/DDoS 所造成的入侵威脅:

DoS/DDoS 通常會搭配 syn-flooding 而造成有效的攻擊[7]，而 syn-flooding 攻擊是依照標準的通訊協定，透過 DDoS 以大量的連結要求，耗費大量的伺服資源。一旦，所有的伺服器資源耗盡，即無法服務正常的客戶，所造成的入侵威脅、威脅等級、脆弱點和衝擊程度的評價，分別是 3、3 和 2。所得到的嚴重程度為 18。

5.2.3伺服器服務風險等級

我們必須透到 5.2.1 所得到的資產總值，和 5.2.2 所得到的嚴重程度，兩個值的乘積即定義為總風險值，透過風險等級表(表 5)的轉換即可得到該資產面對該威脅和脆弱點的風險等級。

以維護不當所造成的入侵為例，由 5.2.2 所得到的嚴重程度為 27，根據 5.2.1 所得到的資產總值為 12，所以得到總風險值是 324。再透過風險等級表(表 5)的換算，可以得到風等級為 C。依此類推，我們可以得到所有的威脅-脆弱點的總風險值和風險等級，如圖 5。

我們定義可接受的風險等級為 D，因此必須針對維護不當(風險等級 C)、病毒感染(風險等級 C)和 DoS/DDoS(風險等級 C)等脆弱點去作風險處理。

5.2.4伺服器服務風險處理

以下，我們將分別說明維護不當、病毒感染和 DoS/DDoS 的風險處理，其中包含控制目標和控制措施。

■ 維護不當

控制目標: 網路區隔，Firewall 佈署

控制措施: 如果一設備上實作太多的功能容易導致人為疏失，單純的網路設計，明確的設備定位，可以避免這種疏失。目前，國網中心所有的服務埠都由 router ACL 管制，因此，我們考慮導入 Firewall，以分擔目前在 router 上的功能。但是，我們中心對外頻寬高達 10Gbps，如果只是在對外出口作 Firewall 設置，可能會導致網路中斷的風險增加，同時，高頻寬的 Firewall 成本較高，因此，我們還必須作網路區隔，將原本分散式網路架構，改成集中式網路架構，並將所有的服務分門別類，根據需求佈置 Firewall。

■ 病毒感染

控制目標: 網路區隔，VPN 佈署，Firewall 佈署

控制措施: 由於作業系統常常會有潛藏的弱點，當被發現後，就會成為新病毒的入侵點。所以，我們必須要將辦公區網段和公開服務網段作網路區隔，並在中間佈置 Firewall，只允許辦公區網段透過開放的服務埠存取伺服器。但是，我們還是要讓格網

小組可以去維護伺服器，因此，我們就佈置 VPN Gateway，讓受到認證的格網成員可以透過辦公區段網路以及網際網路去作伺服器的維護。如此，可以維護的人員受到限制，病毒感染的程度，就可以大幅降低，將風險程度降到可以接受的風險等級。

■ DOS/DDOS

控制目標: Firewall 佈署，拒絕沒有註冊或是私有的 IP 位址建立連線。

控制措施: 我們目前的架構是開放一些特定的公開服務埠，但是 DOS/DDoS 的攻擊，就是針對標準的作業程序作大量的服務要求，耗盡所有的伺服資源，導致無法去服務合法的使用者。如果 Firewall 無法針對這類的攻擊作防禦，那並不足夠，反之，Firewall 必須具備防禦機制[4]，以降低這類的風險。但是，目前這個技術還不是很成熟，有可能會阻斷合法的使用者。因此，我們的另一個考量點，就是去降低攻擊的頻率。我們發現 DDoS 有可能是利用未註冊或是私有 IP 來作攻擊，因此，我們可以在我們的 router 上面加上這樣的限制，讓這類的攻擊頻率降低。

5.2.5伺服器服務殘餘風險

在作完風險處理後，我們必須再回過頭來檢驗脆弱點的嚴重程度。所得到的殘餘風險整理如圖 6。我們可以發現，所有的殘餘風險等級都落在等級 D，可以接受的風險等級內。

資產價值 = 12

威脅點	脆弱點	嚴重程度 = 威脅等級 * 脆弱等級 * 衝擊等級	總風險值 = 資產價值 * 嚴重程度	風險等級
入侵	維護不當	2 * 1 * 3 = 6	12 * 6 = 72	D
	病毒感染	2 * 2 * 2 = 8	12 * 8 = 96	D
	存取控管	1 * 1 * 4 = 4	12 * 4 = 48	D
	DoS/DDoS	3 * 1 * 2 = 6	12 * 6 = 72	D

圖 6 伺服器服務殘餘風險評鑑

5.3 符合可接受風險等級要求的網路架構

綜合上述的風險處理，我們將所有的控制目標和控制項目整合成的網路架構圖，如圖 7。它達到了風險處理的所有控制目標，包含網路區隔、HSRP 1:1 redundant、VPN 佈署、Firewall 佈署。透過控制措施的妥善控制，必可將威脅的發生控制在可以接受的風險等級內。

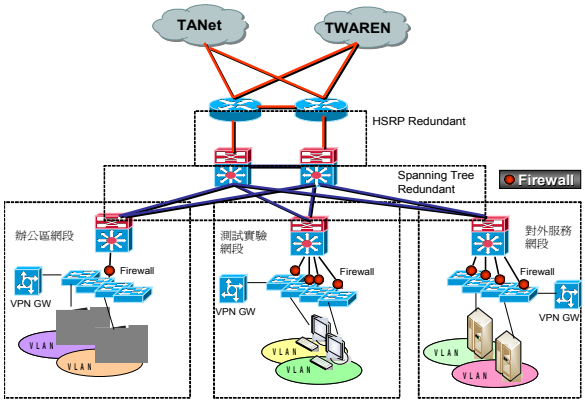


圖 7 綜合所有控制目標的網路架構設計

6. 結論

究竟資訊安全的定義是什麼?什麼樣程度的資訊安全是足夠的安全?在 ISO 27001 所導入的 ISMS 系統的建立過程，從風險的角度，提供了一個系統化的省思和答案。

它將所有的軟體、硬體、有形的、無形的和資訊相關的物件，都列為資訊資產，透過私密性、可用性和完整性評價去作資訊資產的盤點，高評價的資訊資產需要嚴謹的資訊安全保障。同時，計算出風險值，針對高風險的資產透過作業流程，嚴密管理，技術支援等補強方法，降低其風險等級至可以接受的程度。

資訊資產的高低，即是反應資訊安全的價值。透過降低風險至可以接受的風險等級所付出資訊安全成本，即是足夠的程度以確保安全。

在這篇文章中，我們從 ISO 27001 風險管控的角度來建立 ISMS 系統，並以國網中心系統為例，說明風險管理的實務應用。最後得到一個符合國網中心期待的網路架構設計。

誌謝

本文承蒙宏瞻資訊股份有限公司鍾豐智顧問之協助，方能順利完成，特此致謝。

參考文獻

[1] “風險評鑑與風險管理實務課程” ，宏瞻資訊股份有限公司，Oct 2005

[2] Alan Calder and Steve Watkins, IT Goverence: a Manager’s Guide to Data Security and BS7799/ISO17799, Kogan Page, June 2005.

[3] “ BS ISO/IEC 27001 Stand Alone” http://17799.standardsdirect.org/index.htm,Last viewed:Jul/15/2006

[4]B. Xiao，and et al., “An active detecting method against SYN flooding attac”, IEEE Proc. on Parallel and Distributed Systems, Vol. 1, pp. 709-715, July 2005.

[5]Configuring HSRP , http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a008042fbb3.html, , Last viewed:Jul/1/2006

[6] “ Information security and ISO27001 – an introduction” http://www.itgovernance.co.uk/files/Infosec_101v1.1.pdf, ,Last viewed:Jul/15/2006

[7] R. K. C. Chang, “ Defending against flooding-based distributed denial-of-service attacks: a tutorial,” IEEE Communication Magazine, Vol. 40, pp.42-51, Oct. 2002.