小型電子商務業者
資安與個資防護參考指引

財團法人資訊工業策進會

中華民國105年8月

目　次

表　目　次

圖　目　次

壹、指引訂定說明

一、依據

「小型電子商務業者資安與個資防護參考指引(以下簡稱本指引)」係依據經濟部商業司本(105)年度「電子商務兆元推升計畫」之分項工作而訂定。

二、目的

本指引之目的是為小型電子商務業者提供簡明的指引，運用有限的資源，以應付日常面對的資訊安全威脅，協助業者發展電子商務作業之資訊安全環境。

三、本指引參考定位

(一)已建立之安全防護參考指引

1.「交易安全及資安服務平台推動計畫」

針對電子商務交易平台業者，物流商等安全強化指引與上下游安全之自我檢查表，協助平台業者、網路零售業者(使用平台)、供應商及物流商及建立資安防護機制，此計畫提供業者以下規範指引如下：

(1)電子商務交易安全規範-網路平台。

(2)電子商務交易安全規範-供應商。

(3)電子商務交易安全規範-物流商。

2.「資安檢測與輔導計畫」

透過資安檢測技術協助自行架站之電子商務網站透過檢測方式發現網站問題，並提供業者以下規範指引，協助建立資安防護及個資保護能力。

(1)電子商務資訊安全機制與管理規範。

(2)電子商務資訊安全機制查檢表。

3.「電子商務交易安全推動計畫」

提供電子商務業者對於保護個人資料外洩之事前、事中、

事後之防禦及處理機制，以協助電子商務環境健全及安全的發展。

(1)電子商務個資外洩資安防護參考指引

(2)電子商務業者個資外洩資安防護查核表(事前資安強化)

(3)電子商務業者個資外洩資安防護查核表(事中應變)

(二)本指引之需求

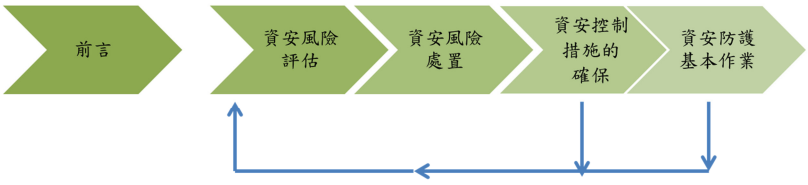
為小型電子商務業者提供簡明的資訊安全指引，以運用有限的資源，應付日常面對的資訊安全威脅。

(三)指引使用限制

本指引之撰寫係針對小型電子商務業者之防禦，並非全面功能性之指引，僅實施本指引所提示之安全功能並無法得到完整的安全架構。

四、整體指引架構

依據本指引之目的，訂定整體指引架構詳如圖 1 所示：



資料來源：本計畫整理

圖 1 整體指引架構示意圖

本指引之整體架構著重目標於「知識建構」，其內容包括：

(一)說明資訊安全之風險管理基本概念與作法。

(二)說明資訊安全之弱點與威脅及其處置措施。

(三)資訊安全風險之個資防護作業。

藉由說明電子商務環境之資訊安全之風險管理問題、威脅及弱點，以協助電子商務業者瞭解本指引中提示之概念、弱點與威脅及其處置措施之必要性與其相對應預防與處理之重點。

五、本指引目標使用者與使用說明

本指引之目標對象為電子商務業者，希透過本指引讓電子商務之經營管理者、系統管理者、安全技術人員及業務人員等瞭解資訊安全與應用於個資防護之重點方向。

六、參考文獻

本指引參考國際及產業標準，藉由引用或參考國際與產業標準及個人資料保護法、網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫，及業務終止後個人資料處理作業辦法等要求，使電子商務業者可以使用標準的作法並遵循法律要求，另外可以作為本指引之延伸，電子商務業者如果有需要進一步的實施全面性的安全措施，也可以經由參考下列本指引參考之國際及產業標準而建立全面性的安全保護作業。

(一)ISO/IEC 27001：2013：Information technology-Security techniques -Information security management systems-Requirements Information technology 為資訊安全管理系統要求，等同中華民國國家標準 CNS27001。

(二)ISO/IEC 27002：2013：Information technology-Security techniques -Information security management systems-Requirements Information technology 為資訊安全管理系統實作指引，等同中華民國國家標準 CNS27002。

(三)ISO/IEC 27017：2015：Information technology - Security techniques -Code of practice for information security controls based on ISO/IEC 27002 for cloud services 為雲端服務基於 ISO/IEC27002 的資訊安全控制措作業規範。

(四)ISO/IEC 27018：2011：Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII

processors 為公有雲個人可識別資訊(PII)處理者之 PII 保護作業規範。

(五)CNS29100：2014：資訊技術-安全技術-隱私權框架。

(六)電子商務(B2C)交易安全規範(包括網路平台、供應商及物流商)，經濟部商業司。(下載網址：http://ec-cert.org.tw/公告訊息→檔案下載)

(七)電子商務資訊安全機制與管理規範，經濟部商業司。(規範索取email：ec-security@mail.cisanet.org.tw)

七、用語與定義

(一)資訊安全(information security）

避免因人為疏失、蓄意或自然災害等風險，運用系統化之控制措施，包含政策、實施、稽核、組織和軟硬體功能等，以保護本組織資訊資產的機密性、完整性、可用性之安全；此外，亦能涉及如鑑別性、可歸責性、不可否認性及可靠度等性質。

(二)資訊安全管理系統（Information Security Management System, ISMS）：

為整體管理系統的一部份，以營運風險導向（作法）為基礎，用以建立、實作、運作、監視、審查、維持及改進資訊安全；等同資訊安全管理制度。

(三)資訊安全管理系統文件

保護組織內資訊資產安全所建立、文件化、實作及維持的程序。

(四)資訊安全管理系統紀錄

遵循安全要求與資訊安全管理系統有效運作的證據。

(五)資訊安全管理系統稽核

資訊安全管理系統之獨立資訊安全檢查，以決定各項活動及相關結果是否與計畫的安排相符，及此等安排是否有效執行及達成目標。

(六)機密性(Confidentiality)

確保只有經授權的人才可以存取資訊。

(七)完整性(Integrity)

確保資訊與處理方法的正確性與完整性。

(八)可用性(Availability)

確保經授權的使用者在需要時可以取得資訊及相關資產。

(九)資產(Asset)

對組織有價值的任何事務。

(十)資訊資產

即指對組織有價值的知識與資料(訊)。

(十一)弱點

是指資訊資產內部可能遭受威脅利用之處。

(十二)威脅

危及資訊資產的外在因素，如天然災害、惡意攻擊等。

(十三)風險

對目標之不確定性的效應。即威脅利用弱點對資訊資產所造成影響之可能性。

(十四)風險擁有者(risk owner)

具可歸責性及權責管理風險之個人或個體。

(十五)風險管理

藉由協調各項活動以指導與控管組織之有關風險。

(十六)風險評鑑

風險分析與風險評估的整個過程。

(十七)風險分析

系統性的使用資訊，以識別緣由與估計風險。

(十八)風險評估

把預估的風險和已知的風險準則進行比較的過程，以決定風

險的顯著性。

(十九)風險處理

選擇與實作措施的過程藉以修正風險。

(二十)資訊安全事件(information security event)

系統、服務或網路狀態被識別出之現象，指出可能係資訊安全政策的漏洞或資訊安全之失效，或先前不知可能與安全相關的情況。

(二十一)資訊安全事故(information security incident)

有顯著機率危害營運及威脅資訊安全之單一，或一連串非所欲或非預期的資訊安全事件。

(二十二)資訊安全事故管理(information security incident management)

資訊安全事故之偵測、通報、評鑑、回應、處理及從中學習的過程。

(二十三)內部稽核作業

由內部稽核小組針對作業程序之安全控制、保護措施、風險評估、營運持續計畫等，進行定期查核，以確保其成效。

(二十四)矯正措施

為避免不符合資訊安全管理制度之事件重複發生，所採取之措施，即消除不符合事項之原因，以防止再發生。

(二十五)預防措施

為預防潛在不符合資訊安全管理制度要求之事件發生所採取之措施，即消除潛在風險之原因，以防止其發生。

(二十六)存取控制(access control)

確保存取資產係依據營運及安全之要求事項授權並受限制的措施。

(二十七)攻擊(attack)

試圖對資產進行毀壞、揭露、改變、使失效、偷竊或取得未經授權之存取或未經授權之使用。

(二十八)間諜軟體(Spyware)

未經使用者許可的情況下蒐集使用者個人資料或其他財務資訊的電腦程式。

(二十九)釣魚(Phishing)

透過偽造的電子郵件、未授權取得之通訊軟體帳號或假冒、被入侵的網站來誘騙使用者交付個人資料、識別資料或財務資料之手段。

(三十)社交工程(Social Engineering)

利用社會關係、人性弱點，應用簡單的溝通和欺騙手段，以獲取個人資料、帳號、通行碼或其他機敏資料並藉由騙取之資料進行下一步驟的攻擊。

(三十一)進階持續性滲透攻擊 (Advanced Persistent Threat, APT)

針對特定組織，經規劃、多方位、長期性的攻擊行為，通常攻擊者為組織型的犯罪組織。

(三十二)資料庫隱碼攻擊(SQL Injection)

攻擊者在正常輸入的資料字串之中夾帶惡意的資料庫 SQL 指令，如果網站程式忽略了檢查，那麼這些夾帶進去的指令就會被資料庫伺服器誤認為是正常的 SQL 指令而執行，因而產生資料庫破壞或資料未授權存取的結果。

(三十三)分散式阻斷式攻擊(DDOS)

攻擊者透過各種手段使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其對目標客戶不可用之攻擊手法。

(三十四)零時差攻擊(Zero Day Attack)

在軟體上發現的安全漏洞，攻擊者在問題尚未被廣泛公布

或提出問題修正之前，利用該漏洞進行的惡意攻擊。

(三十五)跨網站指令碼攻擊(XSS)

是一種網站應用程式的安全漏洞攻擊，攻擊者將惡意程式碼透過資料庫漏洞、系統輸入介面漏洞或其他手法注入或內嵌到正常的網頁上，其他使用者在存取該網頁時就會受到注入的惡意程式之攻擊。

(三十六)源碼檢測(Code Review)

對於原始碼、程式做系統化的檢測審查，通常使用軟體工具掃描或進行同儕審查(Peer Review)的方式進行，其目的是在找出及修正在軟體開發初期未發現的錯誤，提升軟體品質、避免安全漏洞的產生。

(三十七)非軍事區(DMZ, Demilitarized Zone)

是一種安全網路架構的方式，非軍事區網段被建立在不信任的外部網路和可信任的內部網路之間，該網段接受來自外部網路的存取，並允許進行內部網段之存取，這樣區域設立可形成一個保護內部網段而不被外部直接攻擊的安全措施。

(三十八)入侵防禦系統(Intrusion Prevention System)

透過監視網路或網路裝置的網路資料存取或傳輸行為，並與惡意攻擊的模式資料庫進行比對，能夠即時的偵測、中斷、調整或隔離一些不正常或是具有傷害性的網路資料存取或傳輸行為。

(三十九)防火牆(Firewall)

可以監控進出電腦的網路連線，並設定規則以防止惡意人士入侵電腦系統，或者可阻止電腦系統對外進行不當的網路連線行為。

(四十)網站應用程式防火牆(Web Application Firewall)

通常架設於網站伺服器之前端，監視流向網站的 Http/Https 指令要求，透過行為的分析及防禦政策的建立，保護網站伺服器不被惡意攻擊。

(四十一)虛擬私人網路(VPN)

是指在公共的網際網路上，用加密通道及加密方法 建立一個私人且安全的網路，具有保密與認證機制，只有擁有解鎖密碼的相關人員能夠通過身分認證與授權進而讀取資料。

(四十二)遠端控制(Remote Control)

是指利用別處工作的遠端電腦，連線至某電腦進行操作，讓使用者觀察或控制另一個工作階段。而遠端遙控的作法也常被駭客濫用成犯罪工具，例如駭客會藉由植入木馬程式來遙控受害人電腦。

(四十三)自有設備使用(Bring Your Own Device)

一種管理政策，允許組織內的員工或工作者攜帶自己擁有的電腦，或資料處理設備到組織擁有的辦公環境作業，並允許接上組織的內部網路或專有網路的管理方式。

(四十四)弱點掃描(Vulnerability Scan)

弱點掃描通常透過自動化工具，基於已知的系統漏洞或弱點資料庫，針對被掃描的系統做系統化的評估、測試以判斷該系統是否存在系統的漏洞或弱點的方式，弱點掃描範圍包括網路層、作業層、應用系統、資料庫等。

(四十五)滲透測試(Penetration Test)

滲透測試通常由專業的安全顧問以人工方式，模擬攻擊者的思維進行對於系統的攻擊測試，透過利用現有系統的漏洞或弱點，嘗試組合現有漏洞或弱點，並透過測試發現新的漏洞或弱點以達到模擬攻擊的測試目的，找出系統的安

全問題。

(四十六)安全軟體開發生命週期管理(Secure Software Development Life Cycle)

將安全管理、安全需求融入軟體開發流程作業中(例如：在系統分析階段產出系統安全需求)，以開發出安全的軟體。

(四十七)數位鑑識(Digital Forensic)

以周延的方法及程序來保存、識別、抽取、記載及解讀數位資料證據，用以保留數位證據的完整性和正確性，及建構資訊安全事件發生的過程，做為資訊安全事件及司法單位調查判決電腦網路犯罪之依據。

貳、前言

一、電子商務的資訊安全威脅

回顧 2014 年至 2015 年資安相關的新聞，分析後發現透過政府提供 165 的專線通報越來越頻繁，個資外洩所引發的資安事故，涉及到的層次與範圍越來越深入且廣泛，不再只是業餘駭客展現自身實力的測試，而是真正跨國、專業分工、有規劃的組織化攻擊。根據台灣知名防毒軟體科技的統計，台灣是最常受 DDOS/DoS 攻擊的國家名列前茅。2015 年第一季平均每秒可攔截到 1800 個惡意威脅、在行動裝置的惡意威脅更是突破 500 萬大關。在亞洲和衣索比亞更發現已有針對組織的「網路海盜」，面對來自全球各地的攻擊，身處台灣的電子商務業者更需建立起完善的資訊安全防禦策略。

資訊安全經常是部分電子商務業者，會為了降低成本而忽視的防範區塊，也有許多中小組織負責人大多都認為導入 ISO27001(CNS27001)資訊安全管理制度，將增加營運的複雜與麻煩，除了降低整體組織的靈活性，更質疑可能會間接影響業務的發展；實務上，在現行複雜的網路環境中，建立與鞏固資訊安全防禦根柢才是真正基本的營運戰略原則；只要透過政策規範、組織導入管理制度以及教育員工、客戶，自然就可以建立一個安全的網路營運構面，而讓網際網路與電子商務市場可以進入安全防護的正軌。

二、建議的資訊安全管理流程

在本指引內，嘗試利用簡單而有系統的風險管理方式幫助組織進行風險評估，找出各個風險標的和相應的成本、確定需要處理的風險標的之優先次序和選擇適當的風險處置策略（詳見第 3 章）。風險管理的方法不需要一流的風險管理專家所用之專門的方式運算，只需要利用組織的日常知識來做決定即可管理風險，情形就如組織做營業風險評估一樣，組織只需要依據本身需求及資源，思考要做什麼或不做什麼。

在為了減緩資訊安全風險的處置策略方面，本指引提供一些基本管理和技術性的指引，幫助組織建立基礎的資訊安全管理政策與網路安全和控制措施及相關資訊安全風險減緩作業之維護（詳見第 4 章)。而在實行了減緩資訊安全風險之處置策略及資訊安全控制措施之後，為了確保組織在花費的時間、金錢和努力投資的系統與資訊安全管理之有效性不會逐漸落後或退化失效，組織需要一些持續改善的管理機制，本指引會建議一些可行的方案（詳見第 5 章)。

最後，本指引依據主管機關所訂之「網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法」之規定，並彙集上述相關基本資訊安全管理及控制措施，依序展開資訊安全基本防護控制措施的整理，而彙編成「網路零售業資安基本查核表」(詳見第 6 章)，本查核表作業旨在提供業者以資安基本防護基礎進行個資安全防護管理，協助業者因應法規要求，落實個資安全防護，建議業者可參考本計畫，但不以此為限，並考量業者營運風險與需求，訂定符合業者本身營運需求之個資安全防護管理。

三、 資訊安全風險會有什麼衝擊後果

一般人會計算要花費多少成本來降低風險，而不是計算避免了多少風險所帶來的衝擊後果。資訊安全風險可以帶來的衝擊後果太多了，但一般可將它們分類為下列型態：

(一)生命、財產或財務的損失

(二)法律責任承擔損失

(三)客戶流失的損失

(四)組織倒閉

(五)資料毀損的損失

(六)資料外洩(含個人資料)

(七)營運復原的成本損失

(八)破壞商譽及品牌損失

一般組織會大部份都會將損失轉換成財務金錢的損失，同時，每個衝擊後果的類別都有不同程度的損失，例如損失一天的營收和損失十天的營收有很大的分別，而資料外洩更會破壞商譽和客戶流失，尤其是個人資料外洩，尚會面臨法律責任。

部份組織在遭遇資訊安全事故的破壞後，損失了生產力，錯過了交貨限期和破壞了組織的商譽或更進一步致使客戶遭受其他損失(如詐騙)。但組織並沒有意識到這些損失，其實已經變成資訊安全管理成本的一部份，組織並沒有思索一個可減緩資訊安全風險的資訊安全方法，以防止事故再次發生。另外有些組織為追求完全（100 %）排除資訊安全風險而不採取減緩（降低和控制）資訊安全風險的方法，因為組織認為完全排除風險的成本太高，但是沒有充裕資源而最後選擇不作任何行動，造成組織承受極大的資安與營運風險;此作法明顯的忽略了若可以利用低成本、適當的投入資源，亦可得到減緩資訊安全風險的效果。因此使用「省成本作資安，做資安省成本」為原則的減緩資訊安全風險策略，而此策略是可以用低成本的投資而明顯實現減緩風險的效果。

四、資訊安全風險可能的法律責任

在法律要求日趨完善之環境下，組織決對不可以低估資訊安全風險所帶來的法律責任。

(一)法律的遵守

有關電腦犯罪、智財權、個人資料保護等範疇，這些法律牽涉到資訊系統的管理和資訊安全設計，特別是資訊安全管理及資料保護的責任。

(二)疏忽法律的要求

有時組織的電腦資訊或網路系統對其他個人或組織造成破壞，原因是組織沒有做足夠的資訊安全預防措施，而變成不法之徒

之打手。如果因疏忽而直接或間接而持續地造成或致他人的電腦資訊受損，此疏忽可能會成為法律訴訟的根據，例如個資外洩而承擔個人資料保護法的訴訟。

(三)內部人員行為的管控

如果組織沒有做到適當的預防措施，防止員工濫用組織的系統或網路作出違法的行為，或導致另一組織或人員，感到受侮辱或傷害，該組織可能會被調查和訴訟。

(四)個人資料或機密資料外洩

各組織都有法律責任保護保有客戶或員工的個人資料，資料被洩的受害人可向事業目的主管機關申訴，該組織進而接受調查或訴訟。

(五)設備故障對組織的衝擊

電腦資訊和網路系統已經改變了很多組織的運作模式，因此，資訊安全事故可能導致設備故障而不能完成客戶合約合的責任或是組織作業產線停擺，而這些事故會帶來比損失或嚴重的法定責任。

(六)外來非蓄意攻擊的責任

組織的資訊安全漏洞可能會透過網路轉移至另一個組織的資訊系統，例如電腦病毒會攻擊其他電腦，或駭客入侵組織的電腦並利用它來攻擊其他電腦系統而致使他人權益受損。因此，組織的資訊安全衝擊後果，可能還包括其他受害人向組織索取賠償。

五、其他有關資訊安全的問答討論

本指引提出其他有關資訊安全的討論，希望這些討論會令組織相關人員瞭解，如何以正確態度來處理組織的資訊安全風險。

(一)問題：實施資訊安全控制措施不會增加營業收入，同時增加成本，組織為什麼要投資在這方面？

解答：組織決策也許對，但資訊安全控制措施，是在幫助組織

控制風險並幫助組織節省成本(避免損失)。以個人為例，投保人壽保險可以幫個人增加收入嗎？以組織為例，投保營運中斷險可以幫組織增加收入嗎？

(二)問題：實施資訊安全控制措施需要大量的成本，組織根本沒有資源或預算不足。

解答：此點，組織必需要花些工夫做一點研究。請參考問題 4 的解說。

(三)問題：組織內沒有資訊安全方面的人才，那組織要如何做？

解答 1- 修補伺服器的弱點或漏洞，並不需要對相關設施作額外的投資；取消系統不必要的服務，可以降低受資訊安威脅攻擊的機會，也不需要額外的資金。這些修改都不需要專業人士來做，只要透過教育訓練即可達到一定程序的效果。

解答 2- 教育訓練員工，如何利用安全方面處理電子郵件的附件及使用網際網路與社群軟體，降低受威脅攻擊的機會不需要高成本。

解答 3- 善用政府、電子商務資安服務中心(ECCERT)所提供的免費服務、資訊安全資料或訓練 ，有了這些資料或服務，組織就能夠具備基本能力，面對資安事故，並作出更快的應變與反應。

(四)問題：為什麼組織要花十萬元去保護只值二萬元的電腦？

解答 1- 因為重點是要保護組織電腦內的商業或客戶資料，如果組織的資料有很高的價值（比如失去一個產品設計案會令組織損失一百萬元），那麼組織就更應該做一點事。

解答 2- 若組織資源有限，則可用利用 80 -20 管理原則，來處理資訊安全風險，即組織可以用最適當的投資建立控制措施以降低高風險威脅。無論如何作，投資小量成本而將高風險降低，一定都比完全不作為而暴露在更大的風險之下為佳。

解答 3- 資訊安全工作是將風險減緩至組織可以接受程度，而不是完全百分之百的排除風險(此觀念非常重要)，一般而言處置風險之控制措施投資和風險的大小成正比。

(五)問題：組織的電腦都曾經被病毒感染，也沒有什麼大不了！

解答 1- 組織可以認為下次還會這樣幸運嗎？組織有沒有想過最壞的情況？如果這情況再發生在組織會怎樣做？

解答 2- 組織有沒有曾經將病毒傳播至別人的電腦？如果組織的電腦再傳染客戶或合作廠商的電腦，他們以後還會做組織客戶嗎？

解答 3- 請思考購買一套防毒軟體或正版軟體要花多少錢？組織上一次因被病毒感染而損失了多少？組織有沒有比較過這兩個數字？如果被病毒多次入侵怎麼辦？那種狀況成本比較昂貴？

(六)問題：組織資訊安全完全靠技術人員處理。

解答 1- 那很好，有專人幫助組織，雖然技術人員可以幫組織做日常技術支援，但他們不會為組成做風險管理和作出關鍵的決定。

解答 2-組織仍然有機會受到攻擊，組織訂應出快速的應變計畫及改善措施。

解答 3-組織有沒有培訓員工，讓他們更注重資訊安全或更加強專業能力？

(七)問題：組織將資訊安全管理委外給資安廠商服務，組織就可以高枕無憂，不用管理了。

解答 1-恭喜，請外來的專業人員來處理之後，組織便可以專注組織的核心業務了。

解答 2-組織如何確保資安廠商，達到要求的服務水準要求嗎？如果資安廠商停業了，組織的系統會不會就不受控制？

解答 3- 高枕無憂，不用管理? 組織還是需要動腦筋，不然誰會為組織做風險管理呢？發生事故時由誰做決定呢？

參、資安風險評估

一、評估風險的步驟

(一)找出需要保護的資訊資產；

(二)找出各種危害資訊資產的威脅弱點風險；

(三)估計風險對業務的衝擊影響程度；

(四)優先處理高衝擊影響的風險；

(五)選擇和該風險的大小相配的資訊安全減緩策略及控制措施；

(六)找出組織可接受的剩餘風險。

二、確定需要保護的資訊資產

(一)資訊資產是什麼？

資訊資產是即指對組織有價值的知識與資料(訊)，而組織需要用資訊安全方式去保護的標的，它們可以是資訊、軟體、實體設備、人員或服務。

(二)資訊資產分類

資訊資產一般區分為五大類，分別為資訊、軟體、實體設備、人員及服務。

1.資訊資產(Information Assets；IA)：

如資料庫與資料檔案、作業資料庫、系統規劃與設計文件及程序文件、使用與操作手冊、契約與協議、訓練教材、系統文件、業務持續計畫、程式變更、電子郵件及各式紙本或電子紀錄等。

2.軟體資產 (Software Assets；SA)：

如業務資訊系統，含應用軟體、系統軟體、套裝軟體、開發工具及公用程式等。

3.實體設備資產(Physical Assets ; PA)：

如各式伺服器、電腦設備、網路、通訊設備、防火牆、交換機、電話、儲存媒體、行動設備及其他設備等。

4.人員資產(People Assets ; PE)：

如員工、派遣人員、約聘工讀人員及使用組織資產資源之委外廠商人員等。

5.服務資產(Services Assets；SE)：

如支援性內部服務或外部服務、辦公室實體、實體機房、網路服務、ISP 網際網路、語音、照明、空調、電力及消防設施、建築、保護設施、便利設施等。

(三)需要保護資訊資產的那些性質？

資訊資產比實體環境資產更容易在不知不覺間，被濫用和破壞。基本上資訊資產有三方面的性質要受到保護：機密性、完整性和可用性。

1.機密性－確保只有經授權的人才可以存取資訊，即資訊資產的內容不可以讓不應該知道的人接觸。

2.完整性－確保資訊與處理方法的正確性與完整性，即資訊資產的內容應該保持原貌而且不可以被修改。

3.可用性－確保經授權的使用者在需要時可以取得資訊及相關資產，即資訊資產要經常維持可以被即時使用。

每項資訊資產都由這三個性質組合而成。表 1 是一些實例。「 X 」表示該項目的某一性質需要受到特別的保護。

表 1 資訊資產的關鍵性質表

資訊資產	需要保護的性質		
	機密性	完整性	可用性
客戶資料庫檔	X	X	X
組織的營運計畫資料	X		
智財產權資料(軟體設計、作品、音樂美工作品等等)	X	X	
線上交易服務	X	X	X
客戶交易紀錄	X	X	
組織網頁系統		X	X
客戶訂單系統		X	X
產品價格資料			X
中華電信 ADSL 網路服務			X
客戶的交易紀錄	X	X	X

資料來源： 本計畫整理

(四) 如何界定資訊資產？

利用資訊資產分類與作業流程羅列出資訊資產，界定資訊資產一般可以由內部和外部二大部份，其配合資訊資產類別，思考界定。

1.內部資訊資產：屬於組織的資產

(1)實體設備資產之個人電腦、伺服器(主機) 。

(2)實體設備資產之防火牆、路由器、交換器(switch)等網路設備 。

(3)實體設備資產之用來存放,處理或傳送資訊資產的設備，如儲存媒體、行動設備。

(4)軟體資產之各種作業使用之應用軟體、應用程式等。

(5)資訊資產之各種作業使用之資料庫、檔案、文件紀錄等。

(6)人員資產之員工、廠商人員。

(7)實體設備資產之辦公室環境、機房設備。

2.外部資訊資產：

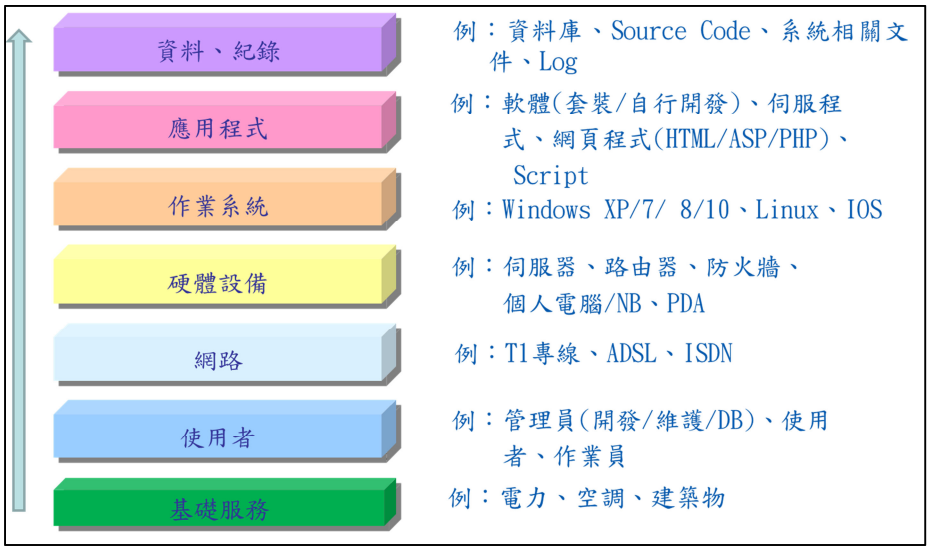
(1)資訊資產之被組織持有但屬於外部人士的資產，例如客戶的個人資料、域名（域名由 ISP 支援時） 。

(2)實體設備資產之由外部人士擁有但可以被組織內部經由網路接觸到的資產，例如通訊線路、域名伺服器。

(3)人員資產之廠商工作人員、廠商提供之服務。

(五) 資訊資產識別方式

利用資訊資產分類與作業流程，並配合下圖由下而上思考各階層之使用資產，進而界定識別出組織之資訊資產。



資料來源：本計畫整理

圖 2 資訊資產思考模式圖

三、確定資訊資產的威脅風險

(一)可能出現的威脅特別多，列舉如下。

表 2 資訊資產的威脅

威脅	說明
實體設備威脅	地震、颱風、火災、炸彈攻擊、涉及飛機或大型交通工具的交通意外、停電、冷氣故障等都對組織的環境和器材造成相當的實體環境破壞。 這些威脅除了破壞實體環境資產，更會衝擊資訊資產(資料和服務)的可能性。
惡意程式碼的攻擊	惡意程式碼類別，包括病毒、病蟲及特洛伊木馬程式。破壞性惡意軟體會利用熱門的通訊工具進行散佈，包括透過電子郵件與即時通訊傳送病蟲、從網站感染特洛伊木馬程式，以及從點對點連線下載遭病毒感染的檔案。惡意軟體也會嘗試刺探利用系統上存在的弱點漏洞，進而無聲無息且輕鬆地入侵系統，並會破壞資料檔案、洩漏資料和降低效率。
駭客入侵	駭客會破壞組織的電腦，例如讓系統當機、偷電腦儲存的資料、竄改組織網頁、利用電腦系統的弱點漏洞入侵、甚而利用組織的電腦攻擊其他電腦，而駭客入侵的後果衝擊將無可預期與後果難料。
拒絕服務/分散式拒絕服務攻擊 DoS/DDoS	亦稱洪水攻擊，是一種網路攻擊手法，其目的在於使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其對目標客戶不可用。當駭客使用網路上兩個或以上被攻陷的電腦作為「殭屍」向特定的目標發動「阻斷服務」式攻擊時，其稱為分散式阻斷服務攻擊（Distributed Denial of Service attack，縮寫：DDoS），這類攻擊會令系統或網路負荷容量超載，令它不能提供服務。DDoS 攻擊可以具體分成兩種形式：頻寬消耗型以及資源消耗型。它們都是透過大量合法或偽造的請求占用大量網路以及器材資源，以達到癱瘓網路以及系統的目的。例如： 1. 用超大量的資料或個人電腦攻擊一個網路或系統。 2. 以分散式拒絕服務攻擊(DdoS)攻擊主機或攻擊 DNS 伺服器以占用組織租用的頻寬、中斷網際網路服務。 3. 用垃圾檔案霸占 FTP 伺服器硬碟容量。
資料庫隱碼攻擊 (SQL-Injection)	資料庫隱碼攻擊是從客戶端輸入的資料中，加插特殊 SQL 指令陳述，並傳送至應用程式中執行所做成，它會組成一項資料庫查詢被執行。駭客可藉輸入變異的 SQL 陳述來改變查詢性質，甚至闖入、竄改、甚至破壞後端資料庫的目的。 攻擊一旦成功，就能讀取資料庫內的機密資料、修改資

	料庫 [如新增/修改/刪除]、執行資料庫的管理動作 [如關閉資料庫管理系統(DBMS)]、回復資料庫管理系統(DBMS)檔案系統內的檔案內容、或在某些情況下向操作系統發出指令等，另外亦可引致很多其他形式的攻擊。
垃圾電子郵件攻擊	發送垃圾電子郵件或夾帶惡意的電子郵件。它會對大量收件者寄送煩人的郵件，通常是不請自來的廣告。垃圾郵件可用來傳送木馬程式、病毒、病蟲、間諜程式及有目標的網路釣魚攻擊，是一大安全隱憂。常見的垃圾郵件形式，是訊息的「收件者：」或「副本：」欄位中沒有您的電子郵件地址有些垃圾郵件可能含有攻擊性語言或不當網站內容的連結這浪費員工的時間和分配給電子郵件的儲存空間及增加被入侵的機會。
釣魚網站或惡意電子郵件	使用虛假網站或聲稱來自某組織的仿冒電子郵件，該等行為均可能涉及詐騙成分。網路釣魚通常是指企圖透過電子郵件、通訊軟體來獲得你個人資訊以竊取你的身份認證。大多數網路釣魚會企圖讓自己看起來像是一般行為，實際上卻是用於犯罪活動。它們看起來就像是來自銀行、信用卡公司、信譽良好的公私立機構的正式通知，通常在訊息中會夾帶惡意連結，引導收件者至看起來與官方極為相似的山寨網站，要求提供帳號密碼等資訊。而惡意電子郵件為惡意人士利用電子郵件(E-Mail)散播惡意軟體（病毒、木馬、後門等程式） 常見的包括仿冒及網域欺騙。 1. 偽冒、詐騙：為了竊取個人資料，利用偽冒之電子郵件，誘騙接收者洩漏個人資料。詐欺電子郵件通常將接收者引導至看似合法的欺詐性網站。 2. 網域偽冒：一般透過入侵領域名稱系統，誤導使用者至詐欺性網站或代理伺服器。
殭屍網路或殭屍電腦	傀儡網路另一個說法是殭屍(Botnet)網路，顧名思義受害電腦一旦被植入可遠端操控該電腦的惡意程式，即會像傀儡一般任人擺佈執行各種惡意行為，當一部電腦成為殭屍網路的一部份時，意味著操縱者(駭客)可將募集到的龐大網路軍團當作機器人來遠端遙控，從事各種非法入侵近年來尤以藉著「網頁掛馬」(入侵合法網頁植入惡意連結）進行資料竊取危害甚遽。瀏覽網頁者在無法察覺的情況下，連線到殭屍網路背景植入間諜軟體等載惡意程式，並從此成為殭屍網路的一員，受到駭客遙控而參與非法活動。一般在電腦擁有者不知情或未授權的情況下，受到駭客或有惡意的人遙控。 電腦會受指使濫發信息或進行分布式拒絕服務(DDoS)攻擊。其中一種常見的攻擊方法是將惡意程式碼(通常

	是特洛依木馬)放進已被入侵的電腦，然後設定等候指令進行攻擊。
員工不小心造成的破壞	以下是員工因不小心而引致的非故意性破壞 1. 錯誤輸入資料。 2. 意外的修改或刪除檔案。 3. 不注意的情況下使用過量的網路流量或大檔案占用硬碟容量。 4. 對其他員工或人士透露機密資料。 5. 對明顯的資訊安全事件的徵兆未予察覺及通報處理，例如病毒入侵，助長攻擊的蔓延。
員工行為不當造成的破壞	行為不當的員工可以利用辦公室的網路做出以下行為： 1. 下載龐大的錄音或影像檔案。 2. 在組織網路伺服器內存放色情照片、非法資料。 3. 用組織的信用在網上購物。 4. 用組織名義發送有侵犯性電子郵件或言論。
惡意員工的破壞	對組織不滿的員工可以對組織做程很大的傷害： 1. 故意下載或使用未經授權的軟體 2. 為了獲得機密資料而竊取資料 3. 竊聽機密訊息 4. 修改已儲存的資料做為欺詐用途 5. 傳送欺詐或惡意的訊息 6. 破壞或刪除關鍵資料 7. 增加電腦和網路的負荷，在關鍵時段使效能降低 8. 發送帶有侵犯性的電子郵件，破壞組織的聲譽
社交工程攻擊	利用惡意電子郵件(釣魚信件/垃圾郵件)欺騙他人，以獲得有用的資訊，造成企業或個人極大威脅和損失的駭客攻擊手法」，通常會用很聳動及時下最熱門的話題當成電子郵件主旨，誘使收件人開啟電子郵件，並自動執行內嵌的惡意程式碼，取得密碼或獲得進入組織系統。

資料來源：本計畫整理

(二)找出威脅和評估它們發生的可能性（一年中發生的機率），即估計威脅的機率。

表 3 威脅的機率範例

威脅	機率
辦公室發生火災	低
鄰近的辦公室發生火災	中
辦公室網路受病毒/惡性程式碼攻擊	高
網路伺服器受駭客攻擊	中
網球連線受到拒絕服務攻擊	低

垃圾電子郵件的攻擊	高
員工不小心造成的破壞	中
行為不當的員工造成的破壞	中
惡意的員工造成的破壞	低
應用系統程式受駭客攻擊	高

資料來源：本計畫整理

四、評估風險對業務產生的後果衝擊

將威脅根據可能性排列，再考慮這些威脅對資訊資產可能造成的後果，換句話說，假設威脅發生後的潛在衝擊，如對電腦系統的影響、對組織的業務的影響、營運損失金額等。

(一)依據威脅發生後的潛在衝擊評估，找出那些威脅最有可能對業務造成最大的破壞。

(二)優先處理高機率及高衝擊度的威脅風險。

表 4 衝擊度分析範例

威脅	機率	衝擊度	衝擊度說明
辦公室發生火災	低	高	營運中斷
鄰近的辦公室發生火災	中	中	影響營運
辦公室網路受病毒/惡性程式碼攻擊	高	高	服務中斷
網路伺服器受駭客攻擊	中	高	服務中斷
網球連線受到拒絕服務攻擊	低	中	服務中斷
垃圾電子郵件的攻擊	高	低	影響營運
員工不小心造成的破壞	中	低	影響營運
行為不當的員工造成的破壞	中	中	影響營運
惡意的員工造成的破壞	低	高	服務中斷
應用系統程式受駭客攻擊	高	高	服務中斷

資料來源：本計畫整理

優先處理的威脅風險為辦公室網路受病毒/惡性程式碼攻擊及應用系統程式受駭客攻擊等二個威脅。

五、選擇風險減緩之資訊安全控制措施處置策略

並非所有的風險的狀態都是一樣，在選擇適當的風險減緩資訊安全控制措施之處置策略時，要考慮它們發生的預期機率和由它們發生後，引起的後果衝擊，其中最重要的原則是：減緩風險的成本永遠不應該高於風險發生導致的損失。

六、找出風險可接受度

資訊安全防護方法可以減緩，但不可以完全排除風險。這些防護方法的效果可以是 ：

(一)降低風險做成的影響，例如安裝滅火器來防止火災蔓延。

(二)降低風險的機率，例如機房遷移至一個較高的地點，可降低受水災的衝擊。

(三)降低風險的衝擊度，例如將重要文件存放在防火保險箱內。

(四)及早提出風險警告可以預先做好防止或補救措施，例如安裝煙霧探測器。

(五)改變風險的性質可以讓組織容易處理它們，例如將機密文件用密碼鎖上，可以將洩露文件內容的風險變成洩露密碼的風險。

風險管理是一個持續的過程，這些重要的風險管理項目會被確認和處理，但建立以後更需要經常重新審查資訊資產、威脅、弱點和衝擊，以及評估是否需要再實行其他控制措施。

肆、資安風險處置

評估過資訊安全風險評估之後，就要透過減緩 (即降低和控制風險) 控制作業，來減輕風險對組織的衝擊。風險減緩處置可分為管理和技術層面，本指引雖然不可能討論所有不同範圍的所有控制措施，但本指引將指出最重要的幾項控制措施。

一、管理指引

(一)資訊安全政策

資訊安全管理的開始起步點是資訊安全政策，資訊安全政策要明確指出組織對資訊安全管理的指示。它要包括：

1.組織實行資訊安全目的，及原則之定義， 以有關資訊安全之所有活動。

2.資訊安全的管理架構；

3.和資訊安全有關的員工的職務和責任；指派資訊安全管理階層之一般與特定責任。

4.實行資訊安全計畫和優先次序；

5.和其他組織或機關單位在資訊安全上的關係。

6.資訊安全政策要符合之下列要求：

(1) 營運策略。

(2) 法律、法規及契約。

(3) 目前與未來預計的資訊安全威脅環境。

(二)怎樣做才算是優良的資訊安全政策？

資訊安全政策可以任何形式出現,它可以是很簡單而且有效的，使用者應該可以從資訊安全政策中找到以下問題的答案：

1.資訊安全政策要由誰參與建立？

2.組織內由誰批准資訊安全政策？

3.誰負責監督這些政策的執行情況？

4.資訊安全政策應通知誰？如何通知？如何確認相關人員已經

接收到且充分了解內容要求？

5.資訊安全政策會何時更新？更新後是如何通知和確認接收？

(三)資訊安全管理人員

組成內要指派資訊安全負責人，資訊安全負責人需負責建立資訊安全政策和監督政策的落實情況。如果組織沒有這個專門職位，這責任可以由管理部主管、財務主管、技術部門主管或人事部主管等兼任分攤。

資訊安全管理功能應該直接向最高管理層報負責，而最高管理層負責批核資訊安全政策，以表示管理層的決心和承擔。

資訊安全管理人員應統籌各部門主管作業政策的落實情況，而各部門主管應該向員工作出適當的說明、執行作業政策和監督，以確保資訊安全政策得以落實。

(四)資訊安全意識教育訓練

資訊安全管理人員應確保資訊安全政策可以有效地通知給每一個員工，而且可以隨時讓員工查詢閱覽，也要負責教育訓練和提高組織員工在資訊安全方面的意識與警覺性，而這些目標都可以透過內部網站、公告欄、員工手冊或教育訓練作業而達到。

安全意識教育訓練應包括以下列部分，並應明文確定：

1.遵守組織資訊安全政策。

2.預防社交工程攻擊。

3.使用網際網路網和電子郵件通訊的最佳作業實務與要求。

4.處理敏感或個人資料之最佳作業實務與要求。

5.每年應接受教育訓練及其時數要求。

(五)以標準、指引和程序步驟實行資訊安全政策

1.人事管理政策

以下是人事單位之資訊安全的幾個重要組成部分：

(1)招聘程序：

申請人的背景接受前必須查核調查。

(2)資訊安全的職務和責任

A.員工必需簽屬組織的資訊安全要求文件，以表示願意承擔義務與遵循。

B.每個組織的資產都應該包括密碼和鑰匙或門禁卡，員工離職的時候必須將這些密碼跟鑰匙或門禁卡交還組織。

(3)在試用期中和已辭職的員工，不應該參與敏感性的工作。

(4)採用有效的方式對員工通知組織的資訊安全政策。

(5)向員工提供資訊安全意識教育訓練，並要求強制參加訓練。

(6)離職程序：

A.離職程序中必需加上取銷該員工對電腦、資訊設施的帳號權限和遠距登入的使用權。

B.離職員工在離開組織當時或之前，應被取銷其進入組織的門禁及電腦、資訊設施的權利。

2.存取控制政策

目的是為確保網路、系統及辦公室應用程式和遠距工作使用之存取管理。

此政策為設計、建立和維護基礎設備提供作業基準。存取控制政策要包括以下幾點：

(1)使用者管理

A.為每一個使用者開設個別的帳戶，目的是分辨每一個使用者和要使用者對自己的行為負責,即一人一帳號，避免共用帳號。

B.為了證明有效身分，執行嚴格的密碼認證管理政策：

a.使用任何資訊系統都要執行密碼認證或更嚴格的認證方式。

b.限制密碼的長度及密碼之強度，如符號、英文大小寫和數字等組合。

c.強制使用者在首次使用分配的密碼登入之後立即更改密碼，以及定期要求強迫變更改密碼。

(2)對關鍵或敏感系統實施更嚴格的認證方式(例如生物辨識)。

(3)實施入侵者禁止和警報機制，以防止暴力攻擊，測試破解密碼。

(4)管制共用帳號和密碼。

3.以最小權限原則管理授權(存取控制)

(1)使用角色為準的存取控制(Role-based access control)管理權限的授權：

A.角色為準的存取控制可以達成「權責分工」(Separation of Duty)的目的。

B.以權責分工或職掌規則界定使用者角色。

C.當一個使用者的職務轉變之後可以較容易更新該使用者的權限。

(2)實行角色為準的存取控制：

A.使用者在組織角色，例如人資部員工、供應商維護員工、管理人員和系統管理員建立不同的使用者群組。

B.經主管同意，設定使用者群組(角色)的使用權限，這些權限要符合僅知原則(Need to know)的最小權限。

C.個別使用者會根據所屬的使用者群組獲得應有的使用權限。如果使用者的職務改變了，使用者應該被轉移至適當的使用者群組。

D.個別使用者有需要獲得額外的使用權限之前，要得到管理層的同意。

4.正確操作使用設備或網路政策

此政策一般由資訊技術部門為組織內部的使用者編寫。它應該界定：

(1)目的和涵蓋範圍。

(2)使用者應該做的事：

使用者須負遵守密碼政策、謹慎地運用電腦和網路資源、以及報告遇到的事故等的責任。

(3)使用者不應該做的事：

被禁止的活動包括：破解密碼、干擾服務、潛入系統、竊聽或刺探在網路上的通訊、與他人共用帳戶、安裝或移除硬體或軟體、透過網路洩露組織的敏感資料等等。

(4)例外狀況的處置作法與條件。

(5)違反政策的後果。

二、應變管理

資訊系統易於受多種外界因素破壞，由較輕的如短期停電、磁碟機故障,以至較嚴重的如設備毀壞、火災及自然災害等也會發生。透過管理、運作及技術控制,大多數的風險及其影響可避免或消除。應訂定應變計畫，以受到災難性破壞時維持關鍵業務活動及系統的運作。

應變計畫可分為許多種，其中最常見的兩種為業務持續運作計畫及復原計畫。業務持續運作計畫著重確保在服務中斷事件發生時，組織的關鍵業務活動仍可持續運作，而復原計畫則提供詳細作業程序以助資訊科技系統的復原。

(一)持續業務運作規劃

持續業務運作規劃涉及訂定業務持續運作計畫，確保在發生人

為事故或天災時，關鍵業務活動能在預定時間內復原至可接受的水準，從而減少對組織造成的損失。實行業務持續運作計畫對每種業務而言，均十分重要。

持續業務運作規劃包括下述五個主要程序：

1.確認關鍵業務活動

如發生事故，組織應了解需集中處理的項目。持續業務運作規劃的第一步，是確認讓組織可繼續營運的最關鍵業務活動所在，故須充分了解業務，包括目標、產品、服務、資源、設施、供應商、顧客及互相影響的因素。

2.評估業務持續運作的風險

無論組織業務規模如何，均可能發生事故，因而應為關鍵業務活動進行風險評估，以確定潛在的風險，並評估會阻礙業務運作的事故所發生的可能性及衝擊影響。

組織應了解會使業務運作嚴重受阻的事故。各項事故均應予以考慮，一些常見的威脅包括：

(1)天災，例如地震、火災、颱風、水浸；

(2)重要設備/資訊系統/設施受破壞；

(3)駭客入侵/資料外洩

(4)對外網路服務受阻；

(5)公用設施服務中斷，例如電力故障；

(6)人命傷亡、疾病、健康及安全問題；以及

(7)恐怖活動及網上攻擊。

3.訂定業務持續運作計畫

業務持續運作計畫可讓組織作好準備，以應付最壞的情況，使業務運作順暢，減少服務受阻及經濟損失。計畫只需加入讓組織繼續營運的關鍵業務活動。

根據關鍵業務活動及潛在風險的分析結果，便可訂定業務持

續運作及復原策略，而選取策略的因素包括業務活動的關鍵性、開支、復原時間及資訊安全要求。

就小型組織而言，業務持續運作計畫可能只是一份安全放置在另一辦公室的文件，內載緊急聯絡資料、資料備份儲存媒體的地點及營運業務所需的其他關鍵物品。

4.批准及實行計畫

在實施計畫前，應進行測試，以確保計畫能有效落實，測試方式可包括模擬、檢討業務運作過程、實作技術復原、在後備地點進行復原程序操作、供應商設施及服務等測試。

在訂定業務持續運作計畫後，應得到管理階層的批准及支持，此節非常重要。

實施業務持續運作計畫期間須注意的事項：

(1)業務持續運作計畫應以正式文件記載，並分發給各相關員工，以提供在事故發生前後及期間之作業依循。

(2)提供教育訓練培訓，讓員工了解業務持續運作的程序、其個人責任及實施計畫須採取的行動，確保各項程序能有效進行。

(3)業務持續運作計畫應存放於安全地點及經常更新內容。

(4)實施業務持續運作計畫以及助機關繼續營運所需的其他物品，例如組織外資料備份儲存媒體，亦應存放於距離組織達一定距離遠的安全地點。

(5)組織可預先與外部組織作出安排,確保能及時回復運作，例如設施接達及電訊系統。

5.定期檢討及持續維修保養

為使業務持續運作安排能符合現況及有效，應定期測試、檢討及持續維修保養。

(1)定期檢討、測試、審查業務持續運作計畫文件及技術方

案(例如每年進行一次)。

(2)假如業務流程或作業環境有新需求或變更，應按需要修訂現行程序。

(3)相關作業程序應納入組織的更改管理計畫內，確保業務持續運作事宜能獲適當處理。

(4)審核及檢討業務持續運作計畫及測試結果。

(二)復原計畫

復原計畫是一套就資訊系統制定復原計畫(DRP)的程序，以復原資訊科技運作設施及相關服務；復原計畫包括一套完善的計畫文件，以處理資訊系統或主機、機房等，因出現災難以致無法運作及資訊全失的情況。

復原計畫應包括詳細的資訊系統備份程序、復原資訊系統的程序(如在另一台電腦場地復原的程序)，以及在災難後資訊系統或主機、機房等復原資訊的程序。

制訂計畫時應考慮資訊系統的機房在災難後可能有一段時間不可使用，且另一機房的資訊系統的運作不能達到理想水準(即可能需要人手操作輔助以彌補降低之服務水準)。

計畫亦應載有一套詳細及經過全面測試的資訊復原及驗證程序，以增加程序的準確性及有效性。此外，應預備用作復原資訊的所需物資及文件，如預先安排在另一機房的遠端通訊網路服務。

應確保各方面都得到足夠的資訊安全保護，並載於復原計畫內，應考慮的資訊安全範疇包括周邊資訊安全措施、入侵偵測系統、防範電腦病毒、安裝修補程式及適當配置系統。

與業務持續運作計畫相似，復原計畫應載有最新資料，尤其是資訊系統出現變更時。

定期的復原演練是測試復原計畫的準確性及有效性的好方法，但由於進行復原演習可能會費時及影響正常操作，組織須根據其業

務環境及需要決定進行演習的頻率次數。

三、建立安全的工作環境

此目的在確保人命和資訊處理設施的安全，實體環境資訊安全措施處理工作環境的資訊安全管制和資訊處理設施的實際使用管制。在任何情況下，減緩實體環境資訊安全風險時的第一考慮都是人命。

(一)環境資訊安全管制

項目	風險和減緩方法
水災	風險 • 水災可能會為電腦、資訊器材帶來災難性的破壞，它可以是來自大雨氾濫或滲漏。 減緩方法 • 用防水外殼保護電腦、資訊器材。 • 將電腦、資訊器材、伺服器設在較高層樓面，而不要存放在地下或地庫。 • 在資訊中心安裝滅火器系統。
火災	風險 • 對付熱源、煙霧和火災的抑制劑(水、滅火器)也可能會對電腦器材帶來災難性的破壞。火災亦會帶來人命傷亡。 減緩方法 • 指派防火監測人員和定期進行火警演習。 • 在器材附近裝置煙霧探測器。 • 在器材附近放置滅火器，並訓練員工正確的使用方法。 • 將資訊備份磁帶存放在防火保險箱。 • 在資訊中心安裝滅火器系統。
溫度和濕度	風險 • 電腦、資訊器材、伺服器需要一個溫度、濕度和灰塵密度受控制的操作環境。 減緩方法 • 將電腦、資訊器材、伺服器安裝在空氣調節 24 小時開啟的房間內。 • 避免將電腦、資訊器材、伺服器擠在狹窄的空間。 • 使用裝有暖氣、通風裝置和冷氣設備的資訊中心。

項目	風險和減緩方法
	• 經常監測和比較實際的規格要求的溫度和濕度。(例如溫度為 10-25℃，濕度為 30-70%)。
電力	風險 • 電力供應時有波動，短暫的不穩定可能會令電腦、資訊器材、伺服器發生故障。 • 電力中斷會令系統停止運作。 減緩方法 • 為重要的電腦、資訊器材、伺服器裝置有線路過濾器的不受干擾的電力供應器(UPS)。謹記在有效期之前更換 UPS 的電池。 • 將重要系統安裝在裝有雙重 UPS 系統和柴油發電機的資訊中心。
其他	風險 • 組織的鄰居可能會為組織帶來問題。 減緩方法 • 在挑選地點時調查鄰近的組織的業務性質，這在資訊中心選址時特別重要。鄰近組織的生產程序、產品和器材的運輸都可能對組織製造外來的風險。

(二)實體環境出入管制

出入管制可避免資訊和電腦、資訊、伺服器被損壞和竊盜的風險。首先，從實體建築物或辦公室外圍的資訊安全設計開始，資訊安全設計的構思。

設計原則：

1.將入口的數目減至最少

2.將實體建築物或辦公室根據資訊安全要求劃分為不同的區域

3.運用多種不同科技和程序的防禦技術

4.監測、資訊安全和登記出入記錄

5.專人陪同進入高度資訊安全區域

實體環境使用管制的優良設計

1.執行身分辨認：

(1)要求所有員工和訪客配戴身分辨認章。

(2)使用員工進出可以令員工對自己的行為負責。

2.在高度資訊安全區域實行更嚴格的身分認證，例如需要使用時額外輸入另一密碼的進出管制。

3.應用最小權限原則；只有負責員工才可以接觸到有關的資產及資訊。

4.管理控制環境(最有效的防禦方法)：

(1)教育員工要注意及提防辦公室的陌生人。

(2)在重要的物業或電腦、資訊器材、伺服器設施上加入資安和登入等安全控制措施。

(3)訪客由人員全程陪同，並在限制區域內的活動。

5.保護好鑰匙和密碼，並執行管制共用鑰匙和密碼的政策。

6.安裝 CCTV 監測敏感區域的入侵者，保留 CCTV 錄影紀錄，提供事後審查或參考。

7.在離職程序中加入取銷離職員工工的所有使用權限及相關系統密碼易動。

四、建立一個安全的網路

辦公室區域網路是一個組織的核心網路。每個員工都使用這個共用的媒介執行作業，例如作業服務、分享檔案、列印、收發電子郵件和瀏覽網頁。

以下是建立一個安全的網路步驟。(本指引將無可避免涉及一些技術性資料。如果理解這部分有困難，請向組織內的技術人員查詢。)

(一)建立一個安全的辦公室區域網路

1.在網路設計時加入資訊安全的考慮

(1)所有資訊安全事項，例如管理政策、技術訓練和委外作業要求，應該在網路設計階段開始時考慮。

(2)選擇資訊設備的時候，要全盤考慮資訊安全的要求。例如：不應該選擇已知有資訊安全漏洞的資訊設備或應用程式，即使組織對它們很熟悉。

2.為網路和系統設計實體環境和環境性資訊安全措施

(1)將重要的資產存放在上鎖的房間機櫃、或其他安全區域內，這包含網路訊號線、路由器、交換器、防火牆和檔案伺服器、主機等，而敏感部門的列印機應放置在該部門內部的房間或在使用者旁邊。

(2)執行訪客使用組織網路、系統或設備的政策。

(3)為內部網路設立私用的 IP 地址

使用私用的 IP 地址可以避免被人從外界的網站進入內部網路。公用的 IP 地址只可用作對外開放的伺服器。

(4)用分區方式設計網路資訊安全模型(根據資訊安全程度將網路分區)，即辦公室-DMZ-網際網路模式。此模式適用於想自己設置電子郵件和網頁伺服器的組織。伺服器被分為兩組，向外的伺服器(外部伺服器)會被放在 DMZ 網路內，同時即使外部伺服器受到破壞，亦只是 DMZ 網路受到影響，辦公室的網路仍然安全。

(5)設計網路結構

設計重點是將伺服器和資料，依資訊安全需要，分配到相關的區域。

A.將防火牆和路由器設定至較佳的資訊安全狀態

防火牆是外圍資訊安全的基本成分。配合資訊安全性高的路由器後，它可以阻擋大部分的外來攻擊。防火牆一定要設置在外來資訊的唯一入口才可以有效阻擋攻擊。如果組織的網路有多個入口，每一個入口都要用類似的方法保護。

a.防火牆和路由器的強化：限制安裝的服務的數目及將管理員密碼加密。

b.確保管理員的進入得到保護：只允許在特定地點進行

網路管理工作及使用加密的通訊道(例如 SSH)進行網路管理工作。

c.為不同的網路介面訂定防火牆規則：關閉不必要的網路服務的進入通道，這可以避免駭客利用這些有漏洞的不必要的網路服務進行攻擊。

d.關閉不必要的網路服務對外的通道。

e.利用網路交換器(switch)代替集線器(hub)連接系統，網路交換器比較不容易被人利用刺探封包資訊或非法架取。

B.將伺服器參數設定至較佳的資訊安全狀態

加強伺服器的作業系統的資訊安全程序。常見的方法包括：移除不必要的服務和軟體、及時修補系統的漏洞、更改預設的管理員名稱和密碼、取消沒被使用的帳戶和使用資訊安全程度較高的密碼。

C.加強應用程式的資訊安全

D.過濾病毒和惡性程式碼攻擊

E.在閘道和個人電腦及主機使用防毒機制

F.記錄資訊安全事故和定期檢閱

G.建立一個安全桌面的標準模範樣式

H.建立備份和復原策略

I.建立安全管理的程序，例如弱點修及補丁(Patch)管理、資訊安全事件記錄監測和更改管理等。

J.保存有關設定和程序的良好紀錄。

(二)建立一個安全的網站

組織決定提供網際網路服務的同時，亦為組織帶來了資訊安全上的風險。降低因提供網際網路服務引起的風險的方法，有兩個方法可以降低這方面的風險：

1.將這部分風險轉至服務供應商

(1)把所有公眾存取的伺服器寄存在網際網路服務供應商。

(2)將部分或全部的設計、實施和維修工作委外給第三者服務供應商。

2.組織建立管理風險的能力

如果組織選擇 1 項，最重要的事項是在服務合約上清楚寫明對服務供應商的管理和服務時限的要求，以及要確保服務供應商提供一個安全的網站服務及雙方對資訊安全責任如何區分及確保安全。

(三)建立一個安全的網站的步驟

建立安全的工作環境、建立安全的網路所討論的步驟適用於建立一個安全的網站。以下是額外要注意的幾點：

1.為線上作業服務提供安全和可靠的管道

(1)如果組織要開展網上交易，必需保證能提供安全的網頁。組織可以採用被廣泛應用的傳輸層安全協議（Transport Layer Security，縮寫：TLS）技術為訊息加密。

(2)組織需要使用由認可的核證組織發出的認可證書在 TLS 網頁上，由認可的核證組織發出的認可證書可以核實組織網址的身分。

2.加強應用程式的資訊安全

3.網路安全措施是必需的，但它們還不足以阻止駭客入侵，因為駭客還會利用網際網路攻擊應用程式的漏洞。

4.幾乎所有應用程式都有漏洞：網頁伺服器(例如 Apache 和 Microsoft IIS)、DNS 伺服器(例如 BIND、Microsoft DNS)、FTP 伺服器(例如 wuFTPD)、SMTP 伺服器(例如 sendmail)和 SQL 伺服器(例如 mySQL、Microsoft SQL 伺服器)、.NET 軟體應用程式、ASP 軟體應用程式、PHP 軟體應用程式等，它

們都有被駭客利用漏洞擊破的紀錄。

5.加強應用程式的資訊安全的方法：

(1)安裝資訊安全修補程式。

(2)強化應用程式的設定。

(3)鎖定應用程式運作的環境。

應用程式在一個限定的環境下以最小權限的使用者模式運作，即使被駭客入侵，也不能得到管理員的權限。

6.定期檢查網站的編碼和腳本程式

除了安裝在伺服器的應用程式外，組織可能在網頁上加上了客戶用的腳本程式和伺服器用的程式。定期檢查這些程式碼，確保它們輸入的資訊在內容和範圍上有效性(為了避免緩衝區滿益和程式碼注入－buffer overflow and code injection)。組織要審核網頁上輸入的要求，以防止不會被轉導傳送到不安全的網站。

7.服務分開為對內和對外

組織可能同時為內部員工和客戶提供電子郵件、域名和網頁服務。可能的話組織應該在不同的主機上操作對內和對外的服務，而且將這些主機分配在不同的網路區域。

8.有需要時使用多重的防火牆

組織可以使用兩重或更多重的防火牆來為對內和對外服務的網路提供更佳的保護，這樣即使駭客成功破壞外層防火牆，仍不能進入最內層防火牆內的網路。建議組織用幾個不同技術的防火牆。例如封包過濾(packet filtering)防火牆加上代理(proxy)防火牆可以提供更廣泛的保護。

9.建立入侵者偵測策略

除了保護系統，組織還需要在入侵者穿過防火牆之前發現他們。無論入侵是否針對組織的服務網路，監控網路入侵的偵

測系統是一個在網路上追蹤入侵者的重要工具。監測主機的入侵偵查系統可以偵測到對伺服器的攻擊，以及尋找對系統檔案未經授權的修改。

10.評估服務供應商的資訊安全程度

部分網際網路基礎建設難免需要由服務供應商提供，例如網際網路連線、路由器、域名伺服器和電子郵件伺服器。這些設備的資訊安全漏洞都可能會為組織帶來衝擊。

11.為資訊安全事故應變做好準備

(四)建立一個安全的無線網路

無線區域網(WLAN)有幾個資訊安全問題：

1.沒有像有線網路的實體環境資訊安全保護。

2.WLAN 設備的資訊安全強度程度不夠。

3.技術本身的資訊安全防護不夠強，加密演算法可能會有資訊安全漏洞。

4.建立一個商業用的安全性 WLAN 的步驟

(1)風險評估

在選擇使用 WLAN 提供重要和敏感的服務之前，組織要先評估 WLAN 的風險。還需要在成本預算內加上額外的管理和資訊安全計畫的費用。

(2)管理政策

A.嚴禁員工擅自增加進入點(Access Point，AP)。

B.嚴格執行員工對維持資訊安全設定，例如密碼、SSID、WPA2 金鑰的責任。

C.教育使用者未經授權而進入系統的法律和道德責任，以及禁止他們連結到其他無線網路。

(3)計畫

A.選擇一些可以升級的方案。選擇一些韌體可以被升級

的 AP 和 WLAN 卡。

B.Wi-Fi 保護利用 WPA2，並加強了認證和加密技術，在計畫時應考慮最有成本效益的技術。

C.選擇一個可以讓組織集中管理的技術，例如自動分發和更新密碼，以及結合組織現存的認證系統。

(4)設計和實施

A.不要使用時將 Wi-Fi AP 關閉。

B.視 WLAN 為不可靠的網路。將無線網路隔離，使用獨立的網路。在有線基建和無線網路之間安裝設定正確的防火牆，以管制進入內部和服務網路的交通。

C.分配靜態 IP 地址(關閉 DHCP)給 WLAN 使用者。沒有有效的 IP 地址的客戶端不可以連接。

D.將 AP 連接到網路交換器(而非集線器)可防止網路流量資訊被刺探。

E.使用媒體存取控制位址(MAC)地址過濾管制進入，只有獲授權的 WLAN 卡的連接，這方法適用於有限數目的 WLAN 卡。

F.選用一些要求使用者先認證才可以使用 WLAN 的認證方案。

G.開啟 WAP/WPA2 加密，並選取較長的密碼為佳。

H.定期更改共用密碼或金鑰，以增強資訊安全。

I.在重要的應用系統或服務上，在 WAP/WPA2 上加上虛擬私人網路(VPN)技術把無線通訊加密。

J.盡可能關閉 SSID 廣播(有些 AP 管理程式的圖像界面有提供此功能，有時被稱為「封閉網路」(closed network))，並通知個別使用者正在使用的 SSID。

K.如果 AP 使用 SNMP 管理，開啟 SNMP 進入存取管制

列表(ACL)，只給予特定人員 AP 管理權。

L.加強預設設定的資訊安全

a.更改預設的 SSID。

b.將預設的管理員 ID 和密碼更改至更嚴密的。

c.如果組織的 AP 是用 SNMP 設定，組織要確定組織已經更改了預設的 SNMP 名稱和族群字串。組織應使用一個較長的和由字母和數字組成的 SNMP 族群字串。

(5)檢討和審查

定期檢查內部或外部的異常 AP。

(五)建立一個安全的遠距工作環境和虛擬私人網路(VPN)

遠距工作讓員工或廠商人員更有效地工作，以及讓系統管理員在辦公室時間以外都可以支援組織的網路。但遠距工作取可讓使用者接觸到組織內部網路及主機的心臟地帶，因此帶來重大的資訊安全風險考慮，所以計畫時一定要小心謹慎。

1.提供遠距存取內部網路對資訊安全提出了幾個技術性挑戰：

(1)如何認證使用者？

(2)如何認證目的系統？

(3)如何確保通訊的機密性？

(4)如何確保通訊的完整性？

目前大都使用虛擬私人網路(VPN)技術回應這些問題，VPN 大致分為 IPSec VPN 和 SSL VPN 二種。

2.遠距虛擬私人網路的優點

(1)VPN 技術可以在不安全的網際網路網路建立一條加密的管道，保護資料的機密性。

(2)在正確的設定下，發訊者和接收者都不可能被偽冒(認證考慮)。

(3)使用遠距VPN可被設定至使用目的系統的私人IP地址，為網路增加一層資訊安全。

3.遠距 VPN 的資訊安全事項

(1)遠距 VPN 並不是全無問題的方案

首先，VPN 保護由手提電腦至 VPN 閘道之間的通訊的保密性，但它不會保護手提電腦免受攻擊。如果手提電腦被病毒或惡性程式碼入侵，或被駭客控制，接通 VPN 之後它可以被用來向內部網路發動攻擊。所以建議：

A.嚴格執行在手提電腦安裝個人防火牆、防毒軟體和防間諜程式軟體的政策。

B.如果 VPN 閘道支援這功能，在授予網路進入權之前先檢查手提電腦的電子郵件程式和瀏覽器的資訊安全漏洞的修補程度，通過檢查才予以放行。

C.VPN 的設定的高度彈性，在某些情況令 VPN 不太安全。例如共享密碼的應用會讓駭客從社交工程或前員工獲得共享密碼之後有機可乘。建議使用動態密碼及其他安全措施來確保手提電腦和 VPN 閘道之認證。

D.VPN 使用者設定中強制使用者連接前先登入。

E.對 VPN 閘道實施最小權限進入控制。

F.員工離職程序中要加入取銷前員工進入 VPN 的帳號權限。

G.如果一個使用者透過 VPN，從網際網路進入內部伺服器，一個加密的管道便會由該手提電腦連接到 VPN 閘道。從 VPN 閘道到內部伺服器的通訊是沒有加密的。

五、加強使用者使用網際網路的資訊安全

以下是一些使用者使用網際網路時經常提出的資訊安全問題：

(一)如何保護組織電腦，免受來自網際網路的攻擊？

1.不要打開可疑的電子郵件及其附件。

2.使用需要使用者帳號登入和密碼的電腦作業系統。這可以防止未經授權的人使用組織的電腦和安裝組織不准使用的軟體。

3.更新作業系統、網際網路瀏覽器、電子郵件程式和其他應用系統的資訊安全漏洞修補程式：

4.開啟 Windows 系統的更新功能和使用 Microsoft Baseline Security Scanner 掃描系統的漏洞。

5.安裝個人防火牆和過濾對外的通道。

6.安裝防毒軟體及定期更新病毒定義檔案。

7.間諜程式和廣告程式大多數都跟隨其他程式一併進入使用者的電腦。這些都是網路上免費的程式。間諜程式會在沒有使用者的同意之下秘密的將使用者的上網活動報告至第三者。另一方面，廣告程式會在該免費程式運作的時候顯示廣告條。

8.間諜程式的問題是使用者自己將它們安裝到電腦上，防毒軟體可能不認為間諜程式是惡意的。

9.不安裝來自不可靠來源的程式軟體。下載之前先查閱該網站的政策、檢查下載軟體，以核實它的來源。

10.安裝防間諜程式軟體及使用最新定義檔案。

(二)如何保護保存在網站的個人資料？

1.閱讀網站的私隱和個人資料政策。

2.不要將密碼存檔在硬碟或系統上。

3.關閉自密碼動儲存功能。

4.將 Cookie 設定至符合組織的需要(在 Internet Explorer，選擇「工具」網際網路選項「私隱權」)。

5.瀏覽器關閉之後刪除臨時網際網路檔案(在 Internet Explorer，

選擇「工具」網際網路選項「進階」)。

6.不要使用公共網際網路電腦，若要使用公共網際網路電腦之後要清除快取記憶體的記憶和瀏覽歷史。

7.不要在公共網際網路電腦輸入個人資料及帳號密碼。

(三)如何避免個人資料被未獲授權使用：

1.保護電腦上的個人資料。

2.訂閱之前先閱讀規則、協定和條款。

3.不要在聊天室和電子郵件透露個人資料。

4.使用不同的電子郵件地址訂閱電子郵件訊息和電子報。

(四)如何處理垃圾電子郵件？

1.避免個人資料被未獲授權者使用。

2.不要回覆垃圾電子郵件，這不能制止它們，況且很多發送垃圾電子郵件的人都用假的電子郵件地址。

3.用不同的電子郵件地址訂閱電子郵件訊息和電子報。

4.用防垃圾電子郵件方案，例如使用在電子郵件閘道或電腦上的軟體：

(1)使用黑名單，過濾垃圾電子郵件的來源。

(2)用垃圾電子郵件過濾器過濾垃圾電子郵件，加強組織的電腦的資訊安全，防止被第三者用來發送垃圾電子郵件。

5.向 ISP 報告垃圾電子郵件的來源。ISP 通常都有專門的電子郵件帳戶處理這些濫用情況。

(五)如何保護通訊的機密性？

如果組織要利用瀏覽網際網路，處理機密或敏感性資料時，建立使用被 TLS 加密的網頁，並將資料加密的傳送到網頁伺服器。

(六)如何做到安全的網上交易？

1.保護組織的電腦免受病毒和間諜程式的入侵。

2.不要選用電子郵件內的 URL 或不可靠的網站的 URL。要進入這些網站時，以人手輸入 URL 或使用之前到過的網站的書籤。

3.避免在公共或資訊安全性低的電腦上(例如咖啡店或圖書館的電腦)，使用網路銀行服務或做金錢上的查詢和交易，這些公共電腦可能被裝上特洛伊木馬程式或監察程式。

4.當使用網際網路做網上財物查詢和交易時，不要同時開啟其他瀏覽器視窗和進入其他網站。謹記將交易紀錄和確認通知列印出來，並保留它們作為紀錄。

5.永遠不要輕易交出個人資料和信用資料。

6.閱讀和瞭解網站的資訊隱私權政策，組織應該可以選擇是否容許該組織使用組織的資料。

7.確保交易通過安全管道進行，盡可能使用較嚴格的加密技術。

六、病毒防護

病毒和惡性程式碼的攻擊已經充斥網際網路，組織需要防止這些攻擊和避免損失。

(一)運用強而有力的偵測和防護技術方案

1.在網際網路電子郵件閘道和檔案伺服器安裝防毒軟體。

2.安裝防毒方案去過濾其他容易受病毒入侵的通道。例如瀏覽網頁、和 FTP。

3.在個人電腦及筆電上，安裝和維護防毒和防間諜程式軟體以偵查和防止病毒或惡性程式碼，開啟實時保護功能。

4.經常更新病毒及間諜程式特徵(又稱為病毒檔案)，建議使用自動更新功能。

5.使用中央管理機制功能，在一個地點管理所有電腦的病毒及

間諜程式特徵更新、掃描時間表、掃描報告和監控被感染狀態。

6.定期掃描電腦的硬碟，以偵測和移除病毒及惡性程式碼

7.執行至少一星期一次的定時病毒及惡性程式碼掃描，這掃描過程可以定在非辦公時間，例如午休或下班時間進行。

8.開啟「掃描全部檔案」選項。不要只掃描程式檔，很多流行的病毒及惡性程式碼都其他檔案形式傳播。

(二)設定防火牆去過濾進出的通道原則(Rule Policy)

1.除非清楚註明容許通過的通道，其餘的進入通道一律過濾禁止存取。

2.限制不必要的對外通道。對外通道的過濾可以有效地阻止大部分的特洛伊木馬程式向外洩漏機密資料。

3.在重要的伺服器安裝檔案完整性偵測軟體，以偵測系統檔案有否被未授權的修改。

(三)將病毒入侵的可能性減至最低

1.限制外來人士(例如在訪客和承包商)的電腦在檢核為安全之前不能進入組織的網路。

2.移除不必要的軟體及服務，很多病毒都攻擊電腦上的軟體的漏洞，例如 IIS、SQL、DNS 服務。如果組織不再需要這些軟體，移除它們可以降低組織受攻擊的機會。

3.儘快修補系統和應用程式，修補軟體(例如作業系統、瀏覽器和辦公室應用程式)的資訊安全漏洞。

4.留意最新的修補資料，例如開啟 Windows 更新功能或訂閱資訊安全的新聞。

5.避免共享文件夾。如果有正當原因必須這樣做時，建議建立目錄權限及使用帳戶和密碼把它保護，同時經常掃描這文件夾有沒有病毒。

6.用最低的權限執行應用程式，可以避免惡性程式碼得到系統管理權限，對系統做成更大的破壞。

(四)建立處理電子郵件和檔案的良好守則

不要完全依賴工具去偵測和防止病毒和惡性程式碼攻擊，使用者的謹慎也是防止和偵測病毒的入侵的關鍵，這在防毒工具未及更新新病毒特徵的時候尤其重要。

1.小心處理電子郵件的附件，不要開啟來歷不明的電子郵件附件。某些病毒或惡性程式碼會假扮成祝賀卡，除非組織能確定附件是什麼，否則不要執行任何附件。

2.使用磁碟、光碟和從網上下載的檔案前先用防毒軟體檢查。

3.不要使用非法的軟體，使用非法軟體是非常危險的行為。這些軟體可以帶有病毒、蠕蟲或特洛伊木馬，安裝非法軟體可能會令組織的電腦感染病毒。

七、系統獲得、開發及維護管理

(一)系統開發一般安全要求

1.資訊系統開發或獲取前，須將資訊安全需求納入考量並獲得核可，並於專案管理作業中實施。

2.資訊系統開發維護作業應區分正式服務環境、開發測試環境，以確保資訊系統、程式與資料之機密性、完整性、可用性與個人資料之要求。

3.防止資訊系統中的輸入資訊錯誤、遺失與未經授權的修改或使用。

4.必要時採用加解密機制以保護資訊的機密性、完整性、可用性與個人資料之安全。

5.系統檔案及資料庫之存取權限，應限制僅被授權者可以存取，以確保其安全性。

6.資訊系統需執行修補程式或關閉不使用之服務，以降低因使

用已公布的資訊系統技術弱點而導致的風險。

7.除了資訊系統自動的安全控制外，亦可加入手動執行安全控制措施。

8.資訊系統相關文件(如該系統之操作手冊/維護手冊)應明確標示資訊安全控制措施（如：備份與回復方式），以利使用者及技術支援人員瞭解系統之安全控制措施。

9.應將資訊系統及資料庫之處理過程記錄於作業或稽核日誌（Log）。

(二)資訊系統檔案的保護

1.對具關鍵或敏感的資訊，應在傳輸或儲存過程中利用加密或其他合宜之措施保護(如數位簽章或訊息鑑別碼)，以確保資訊的機密性、完整性、可用性與個人資料之安全。

2.應遵循組織訂定的資料保密規範，及組織認可的加密或其他合宜之措施，以確保加密技術產品的安全功能。

(三)應用系統安全功能

1.程式開發需使用帳號驗證機制時，除一般帳號密碼外，應考慮使用動態密碼、簡訊密碼或與其他安全驗證機制整合，以確保安全性，如公開金鑰基礎架構（PKI）、授權認證（CA）機制。

2.自訂使用者資料庫存放使用者密碼時應避免存放明碼，在密碼寫入資料庫時考慮利用加解密元件或是用雜湊，以保護密碼不被外洩。

3.應用程式申請使用資料庫系統的 Table，若確定這些 Table 並不需要使用到時，應提出申請予以刪除，以免惡意使用者利用這些 Table 獲取過多資訊。

4.程式設計應對字串的輸入加以過濾，並限制長度，例如單、雙引號都應過濾。

5.針對資料欄位的輸入，如為已知之資料範圍，應提供選單或選項之方式進行輸入。

6.強制進行資料輸入檢查，並限制前端應用程式資料輸入的長度與資料型態(如數字或文字)，另在輸入敏感資訊時應適當使用隱碼功能設計。

7.應用程式應設計各種例外狀況管理（擷取和回傳例外狀況、設計例外狀況案例、傳送例外狀況資訊）與處理機制，以擷取與存錄錯誤資訊，並防止直接顯示原始完整錯誤資訊給予使用者。

8.應用程式應具備檢驗登入身分識別、認證與密碼保護功能(例如密碼長度限制、密碼組合限制、密碼錯誤次數限制與變更密碼歷史管理等)。

9.自行開發或委外專案開發之程式，應進行惡意程式碼之檢查並予以紀錄留存備查。

(四)應用系統資料管理

1.測試系統與正式系統所使用之環境、資料應適當區隔，使用者測試前之測試資料若為真實資料，應應保護測試資料，並將敏感性之資料內容轉換為相同格式之虛擬資料內容或是採取與真實環境相同程度之安全管控。

2.若程式原始碼為組織所有，進行應用程式變更前，應確認現行使用程式版本，並取出現行使用程式版本之原始碼，進行變更之程式開發作業。

3.應用程式變更完成後，應請承辦人或委外廠商提供變更後之程式版本，存放於不可抹寫之儲存媒體(如光碟片)或存入程式庫內管控。

4.測試產品之前，應對程式原始碼進行抽查及評審，必要時執行程式原始碼審查(Code Review)。

(五)為確保安全性與可靠性，委外開發或維護之應用系統，應於合約中明訂下列事項：

1.委外開發或維護之系統，應與委外廠商明訂服務水準協議（Service Level Agreement），以規範支援及維護方式，確保系統或業務的正常進行。專案執行過程發現專案執行效益不彰、政令變更或是委外廠商無法履行合約等不利專案繼續執行之因素時，應依據服務水準協議對委外廠商進行罰則。若專案需暫停或取消，承辦單位須以行政程序辦理專案暫停或取消，並以公文會辦相關單位辦理。

2.作業時如發生錯誤或資料漏失，且確定屬於委外廠商責任時，應由委外廠商負責更正；另外若損及他人權利義務，委外廠商亦須負責。

3.委外廠商對業務上所接觸之資料，均應視為機密並採必要之保密措施，委外廠商及人員，應依組織規定填具委外廠商保密切結書，任何因程式開發洩密所致之賠償及刑事責任，概由委外廠商負責，並列入組織拒絕往來戶。

4.委外廠商於重大之資訊安全威脅發生時應主動提供之維護服務內容。

5.依據業務流程分析結果，要求委外廠商依據系統之重要性訂定維護服務內容，並執行必要的應用系統架構復原演練，維護服務內容至少應包含服務廠商人員資歷、服務時間、問題處理與回覆方式、問題處理時限、系統回復時限與系統備援程序等。

(六)系統技術脆弱性管理

1.應向承辦人員或委外廠商確認相關系統修正或安全問題更新程式之影響與處理方式，以建立應用系統技術脆弱性資訊之取得管道，評估可能帶來之風險。

2.應用系統應定期維護，維護內容應包含應用系統容量、應用系統日誌與資訊安全弱點檢視等等，維護紀錄應進行歸檔保存。

八、委外服務管理

(一)委外服務控制措施之考量選擇 ：

1.識別及紀錄，組織將允許存取相關資訊的委外廠商或供應商之型式，例如 IT 服務、公用設施、財務服務、IT 基礎建設組件等。

2.界定不同委外廠商或供應商之資訊存取型式與授權， 並監視及控制其存取過程及程序。

3.以基於營運需求之最低資訊安全要求和風險狀況與個別委外廠商或供應商協議，其所需資訊與資訊存取型式。

4.實施確保資訊或各方提供資訊處理之完整性之控制措施。

5.明訂發生事故或應變時，委外廠商或供應商與公司之雙方責任，如發生資安事件或個資外洩事件時，雙方的應付責任承等權責分攤；必要時，應安排應變及回復作業程序，以確保資訊或各方提供資訊處理之可用性。

6.委外廠商或供應商之人員，接受必要之資訊安全認知訓練。

7.資訊安全要求及控制措施之情況將由雙方簽署書面協議。

8.管理必要之資訊、資訊處理設施及物品的傳送，並確保整段傳送期間之資訊安全。

(二)委外服務一般安全要求

1.委外廠商應提供負責系統維護、聯絡窗口及電話詢答服務，並解決系統相關事宜，並配合組織相關程序辦理異常排除及通報事宜，如必要應提供駐點服務。

2.委外廠商人員，於執行或支援業務時所獲知敏感之資訊，不得對外透露或以任何型式散播。

3.委外廠商處理個人資料及機敏性資料時應遵守個人資料保護、資訊安全之相關法令及法規以及組織相關規定辦理。

4.委外廠商履行合約所提供之軟體或交付之標的物，需具備合法性，不得違反智慧財產權之規定或侵害第三人合法權益，如有違反事情發生，應由承包廠商負責處理並承擔所有一切法律責任。

5.委外廠商使用之工具軟體、處理作業、維護或異常處理之執行紀錄，組織得視需要查檢或稽核，廠商不得異議。

6.委外廠商如因其員工執行業務之過失，而造成組織損失或傷害，委外廠商需負損害賠償責任。

7.委外廠商相關系統之開發或負責人員離職時，應繳回其所借用之設備、軟體及作業權限。

8.合約完成或終止時，組織所提供機敏性之資訊、資產，委外廠商應依合約要求，歸還組織或銷毀，相關歸還與銷毀之作業紀錄應留存備查。

9.於合約期間出入組織辦公場所時，需依相關規劃換證或申請臨時出入證，除工作場所外，勿隨意於其它辦公場所走動，若需於非上班時間加班作業時，應事先提出申請，以利管控人員出入。

10.委外廠商之人員不得存取未經授權之資訊資產，如因作業需求，需對組織系統或資料進行存取，應依據存取控制管理之相關管理規範辦理。

11.攜帶筆記型電腦、行動裝置設備至組織，應依據通訊與作業管理辦理。

12.若因維護或其它需求須使用特定之資訊環境設定或網路 IP 時，應依據通訊與作業管理辦理，提出申請並由組織權責單位負責配置。

13.委外協議或合約內應明訂作業、使用或服務範圍、雙方之權利義務、維護與管理之作業權責、發生服務中斷或障礙時雙方之作業權責及責任歸屬和緊急應變時雙方之作業權責、作業程序及所應提供之資源、時效，同時組織應定期及不定期查核委外廠商是否確實執行，並留存查核紀錄。

九、備份和復原

不論組織如何努力保護資訊，意外總會發生。備份是防止資訊損失的最後防線。

(一)備份程序若要成功，必需預先做好計畫和準備。在系統設計階段加入備份計畫可以令備份管理更有效。

(二)將關鍵資料集中在資訊安全性強的伺服器內，在此備份可以更有效和有效率。

(三)將系統檔案和資訊檔案分開儲存在不同的分割區，這樣可以令檔案更容易備份。

(四)根據業務持續運作計畫的要求設計復原設定，確定後備電腦可以安裝所需的軟體和連接到備份工具和備份軟體。

(五)界定備份和復原人員的角色和責任。

(六)將備份和復原測試作為日常維護作業的一個重點。

(七)備份過程和監控

1.標示備用媒體的週期數目和磁帶號碼，並加上有效期限。

2.將備份日程張貼在備份控制台附近的明顯位置。

3.根據備份策略建立備份工作定義和日程。

4.進行備份工作和記錄備份活動。

5.檢查備份日誌，確保備份成功，若失敗，則要解決出現的問題，記錄遇到的問題並加以跟進。管理層應該定時檢查備份日誌和備份工作紀錄表。

6.安全地儲存備份媒體；銷毀備用媒體的步驟要符合資訊保護

策略。

(八)復原演習測試

1.一個不能復原的備份是完全無用的，組織一定要確保備份策略能迅速地執行。

2.定期做復原演習。

3.如果沒有改變系統的設定，組織可以每三至六個月做一次系統和資訊復原演習。如果有任何系統、備用軟體或備用工具的改變。建議組織應該馬上做這個測試。

4.檢討備份步驟和技術設定和提出改善的建議。

5.執行這些改善方案。

伍、資安控制措施的確保

一、確保資訊安全和管理審查的重要性

前面的章節已經描述過以下的步驟有：

(一)如何找出一個組織需要的資訊安全控制措施，以減緩風險及改善相關作業；

(二)如何選擇減緩風險的資訊安全控制措施方案和實行方法。

但是，這些步驟是以組織保護系統的角度出發，如果改成用駭客或入侵者尋找組織弱點的角度出發，組織可能會發現之前錯過了的某些事項或疏忽的風險(即為漏洞)，當然，最好是在漏洞被利用而入侵發生之前，組織自已將漏洞找出來並改善之。

漏洞容易在以下的情況出現：

(一)在風險評估階層沒有找出來的風險，或者沒有被給予正確的優先處置次序。

(二)漏洞已被確認並且已提出資訊安全措施方案，但這些措施沒有實施或未落實實施或是已實施但無效。

(三)產品或系統新發現的漏洞，該產品或系統之供應商還未有修補程式。

(四)組織的電腦，網路或系統環境改變或更新，但沒有詳細考慮到相關資訊安全措施的配合。

(五)駭客變得更聰明或有新技術、新攻擊方法。

因此，管理層需要一些管理機制，確保減緩風險的資訊安全控制措施的落實執行，並要評估是否達到預期效果，和找出日常作業過程中可能出現的資訊安全漏洞。以下是管理機制方法：

(一)監測管制與審查：持續地監控組織的資訊安全環境和作出必要的改善行動，以持續改善及維持資訊安全控制措施之有效運作。

(二)有效性量測：針對資訊安全作業項目，訂定各項改善目標，並

且定期檢討與改善，以持續改善及維持資訊安全管理之有效運作，而明確的規範資訊安全目標之管理，可確保各項資訊安全之管理品質及運作效率能持續不斷提升。

(三)內部稽核：查驗組織資訊安全管理之各項作業的控制目標、控制措施、流程及程序是否符合法規、ISO(CNS)標準及組織之資訊安全要求，以確保各項業務能有效運作。

(四)管理審查：用一個獨立的過程搜集和分析資料，以決定資訊安全程度有沒有達到組織管理層的目標

二、監測管制與審查

(一)資訊安全監測管制

資訊安全管制涉及資訊安全範疇內之作業監控和進行要的改善行動，包括：

1.資訊安全政策、標準、指引及程序。

2.員工的角色和責任。

3.存取控制，如使用者名稱及密碼、存取權限等。

4.網路安全，如防火牆、路由器。

5.設備安全，如主機、個人電腦。

6.實體安全，如機房。

7.更改管理控制，如系統更新及密碼變更、存取權限變更等。

8.員工資訊安全意識教育訓練。

9.資訊安全事故應變和處理。

有些最有效的管制可以由管理層直接執行，利用稽核措施以找出違反資訊安全政策的行為，例如：

1.進入辦公室區域或機房的門沒有關好。

2.個人電腦登入後沒有人看管，也沒有設定螢幕保護。

3.個人電腦之防毒軟體未更新

4.電源過度負荷。

5.借出電腦設備前沒有登記。

6.共用密碼。

7.訪客在沒有人陪同之下進入機房區域或接觸敏感的客戶資料或系統。

如果管理層不能確保資訊安全政策得以執行，組織的資訊安全環境會逐漸惡化。另一類的管制是由電腦的自動記錄設施執行。電腦和網路都可以被設定用來記錄資訊安全事故，這些事故記錄對管理層而言是無價的財產：

1.為真實或嘗試的濫用提供預警。

2.提供駭客活動或惡性程式碼攻擊的預警。

(1)在不正常時間有人登入系統。

(2)連續的密碼測試（暴力攻擊）。

(3)嘗試的侵入網路。

3.提供資訊安全事故的診斷及追查資料。

4.對違法行為提出證據。

這些紀錄提供了電腦和網路運用重要的訊息。管理層應該定期分析這些紀錄，並作出匯集分析報告和改善行動。以下是一些和記錄相關的建議：

1.只保留有用的紀錄，例如資訊安全審查的存取紀錄。

2.將電腦設施的時間同步，這樣可以較容易將事故串聯。

3.定期檢視日誌紀錄，發現不正常事件的時候立刻檢驗和通報及匯集分析報告。用工具將記錄自動化。

4.儲存紀錄檔案在一個安全的地點，杜絕未經授權的人閱覽和破壞。

(1)其中一個選擇是將紀錄檔案傳送到另一個資訊安全性高的紀錄伺服器。

(2)使用安全的通道傳送紀錄檔案（不途經不被信任的網路），

以防止篡改和側錄。

5.保護紀錄設定，免受到未經授權的破壞。

6.保存檔案、標記和索引紀錄集，以幫助日後調查。

7.將敏感的紀錄加密保護。

8.保留至少六個月的紀錄，並保存以前的紀錄。

9.循環式記錄媒體要定期更換(如磁帶/USB..等)，以確保不會因為儲存空間不足而使資訊流失。

(二)資訊安全審查

資訊安全審查是風險處置保證的重要一環。它的目的包括：

1.檢核操作、行政和管理事項的資訊安全控制措施，並確保符合資訊安全政策。

2.找出現存的漏洞。

3.考察資訊安全政策、標準、指引、程序和它們在執行上的有效性和符合性。

4.檢討資訊安全措施之後，提出建議和改善行動。

以下是兩種檢討方向：資訊安全管理審查和技術審查

1.資訊安全管理審查：回顧資訊安全政策和程序，並尋找系統的漏洞和可能的入侵點。

2.技術審查：測試和確認資訊安全系統是否符合組織訂下的資訊安全政策，確保資訊安全政策準確地反映該資訊安全系統的規則和容許範圍。

資訊安全審查是一個持續的活動，須定期進行。值得一提的是資訊安全審查只能揭露在某特定時聞資訊系統所存在的風險。資訊安全審查可能需在不同場合和情況下進行，而進行的確切時機則視乎系統需求和資源而定，包括：

1.在啟用嶄新或經過重大升級的系統前進行資訊安全審查，以確保符合現行政策、指引及配置標準。

2.定期以人手或使用工具自動進行審查,以偵測資訊安全漏洞。(即弱點掃描/滲透測試)

3.進行隨機資訊安全審查檢查，以反映實際作業情況。

(三)資訊安全管理審查

為確保資訊安全管理能持續有效地執行,維護員工及客戶權益，以提升服務水準並且達成既定的資訊安全目標；建議每半年應召開一次管理審查會議，必要時得召開臨時會議。管理審查會議審查內容應包含：

1.追蹤過往管理審查之議案的處理狀態。

2.與資訊安全管理制度有關之議題的變更。

(1)營運需求。

(2)組織系統、服務和科技技術等的實際的改變或預計改變的詳情

(3)安全需求。

(4)法令或法規要求。

(5)合約的各項義務。

3.資訊安全績效之回饋，包括下列之趨勢。

(1)不符合項目及矯正措施。

(2)監督及量測結果。

(3)稽核結果。

(4)資訊安全目標之達成。

4.客戶、股東、主管機關等之回饋。

5.風險評估結果及風險處理之狀態。

6.持續改善之機會。

7.資訊安全事故報告

三、內部稽核與有效性量測

(一)資訊安全內部稽核

1.稽核的目的

一般稽核的定義：以有系統的過程，所有針對某項特定活動所進行之獨立調查均可稱為稽核。資安稽核的定義則為就所有資訊實務作業，由稽核人員定期對組織之資訊安全管理，包括資訊資產管理、人員安全、實體安全、網路安全及系統安全等整體安全進行查核，並評估其與資安要求或標準相符合的程度，同時將稽核結果呈報管理階層。

組織管理階層應該決定資安稽核目標、覆核控管程序是否落實、發現現有資訊作業相關之缺失及風險,提出改善建議後，控制風險，確保組織業務之安全性與持續性。

2.稽核工作程序

(1)確認稽核目的及範圍

(2)規劃稽核計畫

A.稽核計畫用以規劃稽核之時程頻率、範圍、項目、人力、資源等，使受稽核單位可據以安排與準備。

B.時參考 ISO27001(CNS27001)及組織內部程序規範，製作稽核查檢表，稽核相關管制目標、控制措施、各過程及程序是否有達到符合資訊安全管理相關程序之規定，並如預期執行。

(3)執行稽核作業

C.以調閱紀錄或詢問之方式，進行作業狀況之查證，確認回答者、程序書與紀錄 (證據)是否一致。

D.若發現不符合事項時，應確實填寫稽核查檢內容，描述不符合事項之狀況。

(4)討論事項/ 稽核報告

A.稽核作業完成後，必須邀集受稽核單位主管及同仁，說明稽核結果與所有稽核時發現之不符合事項。並確

定受稽核單位同仁，對稽核發現之缺失，皆已確切瞭解。

B.依據已確認之稽核查檢內容，彙整為稽核報告。

C.稽核單位依據稽核報告內容，開立矯正措施通知單，並交由受稽核單位之業務權責單位，負責擬定及填寫矯正預防措施，後續改善追蹤及確認由稽核單位負責。

3.稽核時機

(1)每年至少實施一次內部資訊安全管理制度稽核作業。

(2)有下列之情形得執行不定期稽核：

A.當資安事件發生，致使客戶或組織損害時。

B.組織變革、業務調整及管理或系統環境改變時。

C.高階主管對現行作業有所疑慮時。

4.稽核檢核表

(1)可利用附件一資安基本查核表作業

(2)自行編列檢核表，並以個人電腦資訊安全防護、軟體使用安全、網路使用安全、委外廠商管理、伺服器管理、實體與環境安全、資產(個資)盤點及個人資料保護為重點。

5.需針對核缺失擬定矯正預防處理計畫與執行改善措施。

(二)資訊安全有效性量測

1.為什麼需要對資訊安全進行有效性測量?

在資訊安全管理領域，若組織能藉由評估資訊安全管理系統有效性的資訊安全度量，建立可量測資訊安全管理系統有效性的方法，將可協助確認資訊安全管理系統實施現狀與對資訊安全管理目標的考核及持續改善資訊安全管理系統。

2.進行有效性測量需要注意什麼?

進行有效性測量的時候，應該遵循什麼樣的原則呢?

A.有依據：有效性測量的過程中，各項指標的設定一定要有理有據，每個測量的指標都應當能夠具體反映出資訊安全管理的運行狀態，千萬不是為了測量而測量。

B.可操作：一個不能操作或不可行的測量指標是沒有意義的，所以有效性測量指標一定是清晰、明確，具體可行的、可操作的，而同時又是容易收集、不能花費太大的成本的。

C.能比較：有效性測量的結果一定是可比較的，一般利用量化的數值、圖形化的參考來展現測量的結果，以清晰、直觀的觀察到資訊安全管理的狀態趨勢。

3.量測指標之設計

A.量測指標之擬定應以量化為主，如執行次數或更新頻率等數值。

B.量測項目與指標之擬定，應每年期檢討，參酌結果針對量測項目與指標進行調整以確保適切性。

C.資安量測指標範例說明：

a.資訊安全事件與處理結果：發生資安事件時，所有人員均會通報，未通報件數為 0；若為 1 級事件，則於 12 小時內處理完畢。

b.主機、系統弱點掃描結果：弱點掃描，每季執行一次，所發現之高風險弱點，則於 3 天內擬定改善措施或計畫。

4.資訊安全管理測量的最終目的是為保障組織資訊安全，降低資訊安全風險而持續進行與改進的，然後可藉由在量測的方式取得資料、藉由數據進行分析，以發現資訊安全管理當前存在的問題，最終達到組織預定持續運行的目標。

四、定期執行弱點掃描

資訊安全審查多數由外面的技術專家或稽核員執行，但組織也可以自行定期進行弱點掃描評估，以提高資訊安全的保證。定期弱點掃描評估一般由內部員工或委外廠商負責執行，找出潛在的資訊安全漏洞，以助組織避免於或降低潛在的資訊安全威脅。建議資訊安全漏洞評估應該在新系統或大改版之系統上線前、更改系統設定之後及每半年進行一次。

(一)弱點掃描評估

目的：找出、確認和減緩，組織資訊系統的資訊安全程度不足而引致的風險。

行動：

1.包括利用網路資訊安全分析工具掃描系統和網路資產，例如防火牆、路由器、伺服器、桌面電腦和網路列印機與作業系統、應用系統、資料庫，找出已知的資訊安全問題。

2.其他行動有：

(1)檢討資訊基礎建設。

(2)分析管理、實體和程序等方面的控制。

(3)評估重要系統的維護和管理機制。

3.分析和詮釋說明結果。

4.提交一個管理報告(向高階管理階層)及改善建議，包括向管理、技術等建議。

五、外來審查或稽核

外來審查或稽核是一個昂貴的項目。所以進行之前先要回答幾個問題：

1.為什麼組織需要審查或稽核？

2.審查或稽核的目的是什麼？

3.審查或稽核些什麼？

4.找誰做審查或稽核？

5.得到審查或稽核之報告之後要跟進什麼？改善什麼？

外來審查或稽核的目的是借助審查或稽核人員(委外廠商人員)的資訊安全專業知識和客觀性，因此他們找到的資訊安全漏洞應該是組織員工找不到的。

外來審查或稽核的成本可以用以下方法降低：

1.良好的文件紀錄可以減省審查或稽核人員尋找事實和作業的時間。

2.在審查或稽核人員來臨之前確保已盡力增強系統的資訊安全。

3.外來審查或稽核人員可以用這些形式進行：

(1)資訊安全管理整體檢討。

(2)用工具及專業找出資訊安全漏洞。

(一)資訊安全管理整體檢討

資訊安全管理整體檢討是一個整體性的資訊安全審查或稽核，用來決定一間組織現行的資訊安全措施是否遵守組織的資訊安全政策或達到適當的標準，例如 lSO27001(CNS27001)。審查或稽核開始之前，審查或稽核人員應先選定一個標準。審查或稽核的目的是向組織的管理層提供組織整體性資訊安全水準的資料，或者為了外在目的，例如要令客戶放心。審查或稽核項目包括：

1.資訊安全政策、標準、作業指引和作業程序。

2.組織資訊安全之角色和責任。

3.組織資訊安全管理和監控。

4.資訊安全控制措施。

5.資訊安全事故應變作業。

管理要詳細考慮後，才尋求外來的審查或稽核。因為審查或稽

核人員的建議，係基於組織對資訊安全政策知道的詳盡性，所以清楚和詳盡的紀錄文件可以節省審查或稽核尋找資料的時間。

審查或稽核報告，會討論現存的風險處置措施的不足。組織的資訊安全文件應該包括這審查或稽核報告和管理層對跟進及改善事項的決定，並於進行下一階段的資訊安全檢討時，應考慮這報告的內容，並作為下一回合的風險評估和風險處置的一個起點。

(二)發現資訊安全漏洞

找出資訊安全漏洞的方法：

1.系統檢核與資訊安全弱點掃描

系統檢核是從內部接點，找出網路或系統的任何資訊安全漏洞和脆弱環節。資安人員或委外廠商人員應找出是否存在企圖入侵等異常活動，亦應按照組織的資訊安全文件（例如系統安全強化標準）或檢核清單查核系統配置和網路設定，以找出與預期設定的差異。此外，資安人員或委外廠商人員可使用自動化資訊安全弱點掃描工具進行資訊安全弱點掃描，從而快速找出目標主機或網路設備存、網站、系統、資料庫等在的資訊安全弱點。

2.滲透測試

滲透測試包括：

(1)由資安人員或委外廠商人員故意嘗試繞過管制保護措施由外部或內部進入網路。

(2)用不同的掃描技術、攻擊手法技術等測試一個網路、主機、網站、作業系統、應用系統、資料庫的防衛能力。

資安人員或委外廠商人員會用各種方法，例如社交工程去取得非授權的權限。滲透測試應該在安裝或更新防火牆或入侵

偵測系統之後進行。滲透測試為管理層提供一個駭客對組織網路及網站的觀點。測試的目的是以外來者的身份利用不同資料和技術去連接組織的網路及網站，藉此測試組織的網路及網站的防衛能力。

任何形式的滲透測試都會暴露組織的資產，所以管理層必需確保資安人員或委外廠商人員都是可靠的人。測試過程的詳情應該事先說明，例如是否和在那些情況之下才會進行入侵作業與分析。由於滲透測試可能會影響目標系統中資訊的完整性,所以必須為目標系統製作最新的完整系統備份。另外，亦應考慮安排滲透測試在非繁忙工作時間進行以免影響業務的正常運作。

進行滲透測試之前，組織員工應該根據組織的資訊安全政策設計的防火牆規則，並且建立一個有效的防火牆管理制度。

六、檢討資訊安全程序

本指引建議以一個分階段的持續改善方法，進行風險評估、風險處置和確保風險減緩控制處置，持續地改善組織的資訊安全環境。有效的資訊安全管理需要管理層和技術人員的專業知識和經驗。在完成一個循環的資訊安全風險評估、減緩和確保之後，有了累積經驗，以後的工作便容易得多。

管理層應定期進行全面的資訊安全檢討。這些檢討要考慮由負責資訊安全的管理人員所提出的報告和建議，因此管理層應該得到下列資料：

1. 資訊安全紀錄文件。
2. 事故應變處置和報告。
3. 事故應變報告和審查、稽核報告的建議與改善情況。
4. 對組織的系統、服務、運作和環境改變的詳細建議。
5. 外在環境有關資訊安全問題的詳細變化：

(1)新的技術或管理技術。

(2)競爭對手在資訊安全方面的展現。

(3)法律、法規的改變。

管理層於檢討後應該建議：

6. 資訊安全系統和程序的改善方案並支持其作業。
7. 給予軟體、硬體、人力資格及訓練等預算。

陸、網路零售業資安基本查核表作業

一、目的

依據相關法令、法規要求及綜合本指引之相關建議，為使電子商務業者能更簡易掌握資訊安全之控制措施與管理重點，是以將相關要求彙編為資安基本查核表，以利業者參考引用。

二、資安基本查核表作業

本表旨在提供業者以資安基本防護基礎進行個資安全防護管理，協助業者因應法規要求，落實個資安全防護。本表屬於鼓勵業者建立自主管理，建議業者可參考本查核表，但不以此為限，並考量業者營運風險與需求，訂定符合業者本身營運需求之個資安全防護管理。

本表係依據經濟部商業司於 104 年 9 月頒佈之「網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法」(下載網址：http://www.rootlaw.com.tw/LawArticle.aspx?LawID=A040100100006900-1040917)，之規定，依序展開資安基本防護的控制措施，並分類為人員、作業、技術及設備等四大類，共四十項控制措施，並提供作業建議及應注意事項。

相關作業細節與表單，詳附件一。

柒、附件

一、附件一：網路零售業資安基本查核表

網路零售業資安基本查核表

公司名稱：　　查核人員簽名：　　查核日期：　年　月　日

類別	項次	符合	部分符合	不符合	其他	備註	是否需諮詢服務
人員	1						
	2						
	3						
	4						
	5						
作業	6						
	7						
	8						
	9						
	10						
	11						
	12						
	13						
	14						
	15						
	16						
	17						
	18						
	19						
	20						

類別	項次	符合	部分符合	不符合	其他	備註	是否需諮詢服務
作業	21						
	22						
	23						
	24						
	25						
技術	26						
	27						
	28						
	29						
	30						
	31						
	32						
	33						
	34						
	35						
設備	36						
	37						
	38						
	39						
	40						

網路零售業資安基本查核表說明

網路零售業資安基本查核表(以下簡稱本表)係為經濟部商業司委託財團法人資訊工業策進會制定，並由中華民國無店面零售商業同業公會負責推動網路零售者(以下簡稱業者)資安基本防護自主管理，以引導業者建立資訊安全防護。

一、目的：

本表旨在提供業者以資安基本防護基礎進行個資安全防護管理，協助業者因應法規要求，落實個資安全防護。本表屬於鼓勵業者建立自主管理，建議業者可參考本查核表，但不以此為限，並考量業者營運風險與需求，訂定符合業者本身營運需求之個資安全防護管理。

二、使用對象：

國內經營網際網路零售業及網際網路零售服務平台業。

三、如何使用本表：

本表係依據經濟部商業司於 104 年 9 月頒佈之「網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法」(下載網址：http://www.rootlaw.com.tw/LawArticle.aspx?LawID=A040100100006900-1040917)，之規定，依序展開資安基本防護的控制措施，並分類為人員、作業、技術及設備等四大類，共四十項控制措施，並提供作業建議及應注意事項。

本表應由業者指派主管、資訊及資安相關人員，共同填寫本表。

填寫步驟如下：

(1) 依序由第一項至最後一項 (即 1 至 40 題)，以本表之建議控制措施為基準，比對業者本身現行資安防護控制措施作法，將比對後之結果作為自評判斷之依據，擇一勾選符合程度(「符合」/「部分符合」/「不符合」/「其他」)欄位，查檢結果若有後續協助需求，請在「是否需 EC-CERT 後續諮詢服務」欄位打勾。

(2) 填寫說明如下：

第 5 項次之 建議控制措施	符合	部分符合	不符合	其他	是否需 諮詢服務
員工和廠商人員，在被允許存取資訊處理設施之前，均應簽署機密性或保密協議。	符合建議控制措施作業說明第 1、2 點，請打∨	只符合建議控制措施作業說明第 1 或第 2 點，請打∨	建議控制措施作業說明第 1、2 點均不符合，請打∨	其他因素或作法說明，請打∨	需後續諮詢服務，請打∨

本表填寫後，請回傳至中華民國無店面零售商業同業公會(e-mail:nemos@cnra.org.tw)。

(3) 在「是否需諮詢服務」欄位打勾，將由中華民國無店面零售商業同業公會及 EC-CERT 技術團隊主動聯絡業者，提供相關諮詢。

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅以舉例做參考說明)
人員	1	指定專人負責資安及個資保護政策、計畫與管理之工作事項，訂定相關程序文件。	§3-3	(1) 正式對內部發佈人令，指派資訊主管或營業主管負責推動資安及個資保護之工作，包括委外作業之聯繫與處理。 (2) 資安及個資保護之政策或手冊文件其對內部發佈(公告或 mail)，向員工及廠商說明要求遵守。(政策或手冊內容包含營運作業要求、資訊安全要求事項及委外契約要求)
	2	檢查同仁存取關鍵服務、客戶資訊，客戶要求的內容已納入安全管理責任並正式授權。	§12-1	(1) 檢查所有公司人員之職責，針對組織之重要服務流程，建立相互勾稽之流程，避免選手兼裁判之授權。如甲受理接單，則由乙審核訂單、再由丙出貨，同時甲乙丙之帳號權限及負責作業之內容不一樣。 (2) 處理個資檔案之人員，其職務如有異動，應將所保管之儲存媒體及有關資料列冊移交，接辦人員除應於相關系統重新設定密碼外，應視需要更換使用者帳號。
	3	每年至少執行一次公司員工資訊安全及個資保護認知宣導訓練。	§16-1/ §16-2 §19-10	(1) 訂定公司年度訓練計畫，條列那些人要接受訓練?訓練課程是什麼?訓練時間? (2) 每年對公司所有員工至少執行一次資訊安全及個資保護認知宣導訓練。 (3) 每年應對公司個資專責人員及資安人員至少執行一次資訊安全及個資保護之專業教育訓練。 (4) 教育訓練後要考試測試，提升員工資安及個資保護之重視。 (5) 教育訓練可自行安排或如參加 EC-CERT 提供的資安教育訓練課程
	4	每年應對公司個資專責人員及資安人員至少執行一次資	§3-4 §16-1	

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅以舉例做參考說明)
		訊安全及個資保護教育訓練。	§16-3 §19-10	或其他專業資安或個資保護課程。
	5	員工和廠商在被允許存取資訊或設施之前，均應簽署機密性或保密協議。	§12-4	(1) 員工和委外廠商在人員報到或服務合約簽署時，應簽署機密性或保密協議書，如切結書、軟體使用規定、網際網路使用規定等。 (2) 所有紀錄要留存備查。
作業	6	依據營運要求，訂定「個人資料保護管理」、「資訊安全政策」、「個人資料檔案安全維護計畫」及「業務終止後個人資料處理方法」等管理程序文件及管制措施並定期審查檢討。	§3-1/§3-2 §5-1-3 §6-1/§7-1 §9-1/§11-1 §15-1 §18-1 §19-2-3 §20-1-2	(1) 資安及個資保護政策制定與修改必須由公司的高階主管宣布，讓員工瞭解規定很嚴謹，公司很注重。 (2) 至少每年一次，由公司的高階主管召開會議，於會議審查檢討文件內容及管制措施的效果並提出改善建議。 (3) 對個資或機密檔案之資訊安全處理原則與程序，應至少涵蓋下列內容： i 檔案於人員個人電腦或工作桌面之暫存或儲存或複製。 ii 檔案於人員個人電腦或工作桌面之刪除或銷毀。 iii 檔案進行內外部傳送時之資料加密或書面彌封。 iv 可攜式儲存裝置(包括 USB 隨身碟、行動硬碟、手持媒體及通信設備等) 之使用限制與管理。 v 保有檔案之儲存與備份。

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明(本說明不是控制措施之標準或全部作法，僅以舉例做參考說明)
				vi 保有檔案之刪除與銷毀。 vii 保有檔案之內外部傳送。 viii 保有個資檔案之處理紀錄管理。
	7	客戶之個人資料及客戶交易檔案，每年至少執行一次清查工作並定期審查維護。	§6-2/§6-3/§6-4	(1) 建立資料或檔案之盤查及審議之管理程序。 (2) 每年由高階主管及相當人員共同查核檢討一次。 (3) 查核檢討若不符合管理程序，則需通知主管，並立即處理改善並加強訓練。
	8	建立帳號管理，包含帳號權限之申請、開通、停用及刪除並定期清查帳號權限，不得有共用帳號之行為。	§ 12-2/ § 12-3 §15-2 §19-7	(1) 建立帳號權限之申請、異動修改及刪除之管理程序。 (2) 每半年由高階主管及相當人員共同檢查帳號權限，並將帳號權限列冊管理。 (3) 帳號不能多人共同使用(二個以上之人員，使用同一帳號)，若一定要用則要有其他保護措施，如值勤表或使用登記表等輔助。 (4) 非專責處理特定個資者不得具有存取或查閱個人資料之權限。
	9	硬體設備、應用軟體及系統軟體等之最高權限帳號應列冊保管；最高權限帳號使用時須先取得權責主管同意，	§ 12-2/ § 12-3 §15-2 §19-7	(1) 針對網路設備、防火牆、系統、程序及資料庫管理者(含設定參數)之特權帳號權限，建立申請修改及刪除之管理程序且其帳號權限需通過主管核准。如主機系統、資料庫及防火牆等管理員之帳號需通過主管核准。 (2) 將所有的特權帳號權限列冊管理，並每半年由高階主管及相當人員共同查核檢討一次。

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明(本說明不是控制措施之標準或全部作法，僅以舉例做參考說明)
		並保留稽核及審查紀錄。		(3) 所有特權帳號權限之申請修改及刪除之紀錄要留存備查。 (4) 所有的帳號之存取使用紀錄，要留存至少三個月並每季審查，若不符規定則通知主管，並立即處理、改善及加強訓練。
	10	超過所規定之預期閒置時間或使用期限，系統應自動將使用者登出。	§15-1	(1) 當使用者登入系統後，若於 15 分鐘內沒有任何作業或訊息交換，則系統即需主動將其登出強制離線。
	11	資訊系統管理者應保存可識別存取來源的稽核軌跡，並定期審查使用者帳號活動，若發現帳號不正常使用時，應回報管理者及主管。	§15-2	(1) 建立應用系統使用權限管理程序，如申請帳號及使用方法、權限設定方法等。 (2) 留置使用者之使用紀錄，內容要有何人帳號/何時登入及登出時間/IP 或設備名稱位置/存取資訊或使用功能等使用資源。如紀錄甲員工利用 ast1 帳號在 1050404am1000 使用 192.168.1.20 之 host1 電腦，使用 ERP 系統查詢訂單 A0001。 (3) 應用系統使用者之使用紀錄，要留存至少三個月並每季審查，若發現不符規定之紀錄，要通知主管，並立即處理、改善及加強訓練。
	12	避免使用未經授權之電腦程	§15-3	(1) 不要使用沒有版權之非法軟體。 (2) 使用免費自由軟體，要檢查取得來源是否安全。使用安裝前應經防

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅以舉例做參考說明)
		式，及其他可能涉及侵害智慧財產權之行為。		毒軟體掃描是否安全。
	13	建立並遵循電子郵件使用安全管理作業之規定。	§15-1	(1) 建立電子郵件使用管理程序，如申請帳號及使用方法、設定電子郵件密碼長度及如何保護電子郵件等。 (2) 執行安全檢查作業，如每季作社交工程(即利用假電子郵件，測試使用者之安全認知是否落實)，若不符規定則立即改善並加強訓練。如員工使用電子郵件必須完全了解社交工程攻擊手法，不得輕易開啟附檔。
	14	建立並遵循使用者通行碼管理之作業規定	§15-1	(1) 建立密碼管理程序，如檢查及使用方法、設定密碼長度、多久變更一次及如何保護密碼等。如要求密碼必須謹慎使用，不得告知其他人、至少每三個月必須更換一次密碼等。 (2) 執行安全檢查作業，如每月作 PC 之安全檢查，若不符規定則立即改善並加強訓練。
	15	個人電腦及主機應有即時掃描及攔阻病毒之防毒軟體，並隨時更新病毒程式碼。	§15-3	(1) 個人電腦及主機要裝設防毒軟體並設為自動更新病毒程式碼。 (2) 建立防毒軟體管理程序，如檢查及使用方法、不得移除等。 (3) 規定每週定期掃描檢查電腦和儲存媒體。

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅以舉例做參考說明)
	16	定期進行設備、系統元件、資料庫系統及軟體漏洞修補。	§15-3	(1) 對使用中之設備、系統元件、資料庫系統、作業系統及工具軟體等漏洞，進行自動更新修補作業，如 WINDOWS /ADOBE /OFFICE /MYSQL /MSSQL /ORACLE /CISCO/JAVA/.NET/防火牆…等軟體更新。
	17	建立並遵循媒體及可攜式儲存媒體使用安全管理作業規定。	§13-1	(1) 建立媒體及可攜式儲存媒體使用管理程序，如磁帶/USB/燒錄機/隨身硬碟/記憶卡等設備之開放權限原則及查核機制。如公司只能使用公司專屬式可攜式儲存媒體，不得私自攜帶使用；要使用 USB 埠，要正式提出申請並經核可後，方能使用。 (2) 機密性資料，若存放於媒體或可攜式儲存媒體上，應該使用加密技術保護資料，如檔案用密碼保護後再儲放至 USB 儲存媒體。
	18	資訊系統及設備僅開啟必要之網路、服務、程式及通道，使用者僅能存取已被授權使用之網路、服務、程式及通道。	§14-2 §15-1	(1) 建立網路連線管理程序，如網路連線權限之申請、開通、修改及刪除等要求。 (2) 建立網路連線之安全需要規定，如網站網路連線服務只能由 80 通道進出，其餘通道要關閉。
	19	使用遠端連線應使用強度足	§13-4	(1) 建立遠端連線之管理程序。如使用何種協定連線交換資料?遠端權限之申請、開通、修改及刪除等要求。

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明(本說明不是控制措施之標準或全部作法，僅以舉例做參考說明)
		夠之加密通訊協定，不得將通行碼記錄於工具軟體內。	§15-1	(2) 使用 VPN/HTTPS 設備或 SFTP 通訊協定連線交換資料。 (3) 帳號密碼不得儲存於系統或工具軟體內。
	20	資訊系統、個人資料、重要資料(資料庫)及軟體應定期備份，並定期執行回復測試。	§13-5 §19-6	(1) 每日備份最好，至少每週要備份一次，備份檔案要保留三週以上，再覆蓋刪除；備份檔案要離線保存。如將備份資料檔案儲存至光碟片或可攜式儲存媒體上並置於安全區域。 (2) 備份資料要檢查是否正確成功。如將備份資料檔每季抽查讀取內容是否正常。
	21	確立與營運所在地之警察機關、主管機關及 EC-CERT 等相關機構之聯絡機制、資安事件管理文件及紀錄留存。	§8-1-5 §19-8	(1) 建立發生狀況時的通知管理程序，如通知誰?如何通知 ?時限為何?等等。如發生事故時，發現人要在 2 小時內電話通知課長及經理，經理要立即通知總經理。 (2) 建立發生狀況時的處理作業管理程序，如誰作何事? 如何執行 ?如何回應?如發現人要現場處理，課長及經理要支援或通知廠商及 EC-CERT 協助或向警方報案。 (3) 相關作為製作成紀錄並留存備查。
	22	服務或設備委外時，應事先明確訂定作業目標、範圍及雙方權利義務。	§11-1 §13-2	(1) 避免允許系統服務廠商以遠端登入方式進行牽涉個資或機密的資訊系統維護或其他有關之運作；若需使用遠端登入方式進行維護，則應透過加密方式進行（如：HTTPS、SSH 等）。 (2) 檢視處理作業委外合約或其他正式文件內容，需至少包括下列要求：

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅以舉例做參考說明)
	23	確定委外廠商之各項安全措施可以符合資料安全及個人資訊保護等法令法規。	§11-1 §13-2	i 乙方(受託人-廠商)應建立個資保護及資訊安全政策，並遵循甲方(委託人-電商業主)的個資保護及資訊安全要求政策。 ii 乙方及其服務人員應簽署之保密承諾。 iii 乙方應對個資保護及資訊安全之處理作業人員進行相關教育訓練(如應在 XX 月 XX 日前，至少受過 X 小時的個資管理與安全維護訓練課程)。 iv 乙方欲將受託之處理服務作業再進行轉包，應事先取得甲方之正式許可。 v 乙方欲將受託之處理服務作業再進行轉包，轉包丙方(受託人-廠商之協力商)亦應符合甲方之合約條款、個資管理程序及安全維護要求。 vi 當契約終止時，相關之個資及作業資料應被銷毀或交還甲方。 vii 規範履約過程中，甲方可適時監督與稽核乙方之相關作業(包括進行考核測試、現場稽核、教育訓練，或其他可行之監督方式等)。 viii 倘因乙方違反個人資料保護法而遭任何其他第三人向委託機構主張任何權利、請求、索賠或訴訟等，除因甲方之故意或重大過失行為所致者外，乙方同意補償並確保甲方(包括甲方人員)不遭受亦不負擔任何索賠、責任、費用及損失。
	24	委託契約內容應包含資訊處理方式、安全政策保護及個人資料保護相關事項之管理及檢核。	§11-1	

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明(本說明不是控制措施之標準或全部作法，僅以舉例做參考說明)
	25	定期稽核及審查責任範圍內的資訊設施與安全政策、標準及其他任何安全要求的遵循性，並保留相關紀錄。	§7-3 §18-1-4 §19-11-12	(1) 將所有的資訊安全及個資防護之作法彙整並至各單位評估執行狀況，並每半年由高階主管及相當人員共同查核檢討一次評估結果，相關紀錄並留存備查。
技術	26	機敏性資訊傳輸過程得採取資訊加密保護措施，資料傳送以業務所需之最少資料為原則。	§13-3 §13-4	(1) 資料在網路傳輸與儲存必須加密。如網站傳輸採取 HTTPS 之保護措施，讓網路通訊資料加密，變成亂碼。 (2) 網站資料或資料庫加密之保護措施，讓資料加密，變成亂碼。如資料利用 zip 加密、或 OFFICE 之密碼加密、資料庫可利用工具或程式設定進行加密。 (3) 要傳輸或儲存之資料欄位內容，以可以完成服務之必要資料即可。如傳輸或儲存資料內有出生年月日，以作為未來生日禮之行銷用，此時只需要傳輸或儲存月日就可，不要傳輸或儲存出生年。 (4) 雙方連線時，應利用帳號密碼及動態密碼或鎖定網路 IP 位置作身分及設備之確認。 (5) 動態密碼可使用簡訊或硬體式設備。
	27	採取具備資訊隱密性功能與識別、確認對方端末設備及防止儲存資料外洩等資料保護措施。	§13-3 §13-4	
	28	明訂網際網路作業相關管理辦法、作業規範及網路系統	§13-4 §15-1	(1) 訂定網際網路作業使用管理程序，例如：如何申請上網權限? 要安裝何種軟體才可上網? 那些網站不可用? 及網際網路使用之安全要

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅以舉例做參考說明)
		安全政策，並定期檢視修訂。		求等。如公司內網對外使用網際網路之人員管理。 (2) 使用管理程序要有審議檢查之控制。如公司使用網際網路之使用率。
	29	建立網路安全架構，於電子商務網站服務網段(主機區)建立防火牆或路由器設備，區隔外網區、DMZ 區以及內網區，並遵循防火牆安全管理程序規定。	§13-4	(1) 利用防火牆或路由器設備，將網路區分為外網區與內網區。 (2) 外網區供客戶使用，內網區供公司同仁使用。 (3) 外網區的通路，要管制。如誰可以連線?用什麼方式連線。 (4) 外網區與內網區之間的通路，要管制。如誰可以內到外連線?誰可以外到內連線?用什麼方式連線。 (5) 訂定外網區與內網區之使用管制程序。如利用連線申請單控制。
	30	至少每年實施 1 次弱點掃描，並完成缺失改善。	§15-3	(1) 針對主機、設備及 PC，每年實施 1 次弱點掃描(1 次為 2 循環)。 (2) 弱點掃描作業後會出報告(第 1 循環)，報告之問題，要改善，改善後再作一次弱點掃描(第 2 循環)。 (3) 報告要視為機密文件，妥善保管。
	31	應避免採用已停止弱點修補或更新之系統軟體與應用軟體。若一定要採用，則應採	§15-3	(1) 不要使用不被原廠支援的作業系統如 Windows XP / WINDOWS SERVER 2000 /WINDOWS SERVER 2003 等，因為原廠已停止服務之軟體。若非用不可，則要採取不可上網之隔離保護或其他配套措施。

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明(本說明不是控制措施之標準或全部作法，僅以舉例做參考說明)
		用其他配套防護措施。		(2) 使用中之相關軟體，要隨時與原廠保持修補、更新作業。
	32	應管制個資檔案透過輸出入裝置、通訊軟體、系統操作複製至網頁、網路檔案或列印等方式傳輸，並應留存相關紀錄軌跡與數位證據。	§15-5 §19-1 §19-5 §19-9	(1) 管制 USB/FAX/MAIL/印表機/FB/LINE 等設施之使用權限申請管理或利用工具管制權限。 (2) 對連線存取紀錄，應至少每季查核檢討一次，若有發現異常，應立即通報主管處理，立即改善並加強訓練。
	33	限制外部網路存取功能，同時外部網路可以存取的機器設備應維持在最少的數量並定期審查檢討。	§13-4 §14-2 §15-1	(1) 針對具有可從外面連線至公司內網之廠商及公司內部人員，建立上述人員帳號權限之申請、修改及刪除之管理程序並記錄帳號、登入、登出時間及 IP 位置。 (2) 將系統或設備之所有的帳號權限列冊管理，並至少每半年由高階主管及相當人員共同查核檢討一次。 (3) 對連線紀錄，應至少每季查核檢討一次，若有發現異常應立即通報主管處理。
	34	建立存取控制(即帳號權限管理)機制功能，加強對不當	§15-1 §15-5	(1) 建立帳號權限之申請修改及刪除之管理程序。 (2) 將所有的帳號權限列冊管理，並至少每半年由高階主管及相當人員共同查核檢討一次。

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明(本說明不是控制措施之標準或全部作法，僅以舉例做參考說明)
		資料檔案及存取之檢查。		
	35	應確認資訊系統開發設計中已納入必要的安全控管機能。	§15-1 §15-2 §15-4	(1) 資訊系統要開發或修改時，除功能需求外，需針對資訊安全列入要求並落實作業。如密碼一定要 8 碼以上，若未設定為 8 碼，則予以卡關，不能到下一步、如要求網站要在 HTTPS 的通訊加密作業環境等。 (2) 資訊系統/作業系統/通訊軟體等所應用之軟體版本，開發設計時應避免該軟體版本已知弱點或已經有安全處理。
設備	36	應建立公司資訊設備清冊並定期盤點及檢討資訊設備的安全防護機制。	§14-2	(1) 每項設備必須有管理員負責保管，並有設備財產清冊，登記規格資源、服務用途、裝設軟體及 IP。 (2) 每年度或半年度執行設備財產盤點作業，並更新設備財產清冊。
	37	識別所有資訊資產之擁有者，並指派維護資訊資產責任。	§14-2	(1) 各類設備財產指派人員負責保管。 (2) 訂定設備財產之保護要求，例如：筆電、客戶資料表等不用時收到櫃子並上鎖等。 (3) 指定專人負責管理儲存個人資料檔案之資訊設備與其他相關設施等，並檢視、處理其錯誤或異常事件等訊息。
	38	所有主機及設備在接入網路	§14-2	(1) 無論是新購或重新安裝之主機及設備，在正式上線提供服務之前，應檢查相關參數之設定值是否安全，並與廠商交接帳號密碼。

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅以舉例做參考說明)
		前，應變更供應商預設之帳號或通行碼，並移除非必要之所有帳號。		(2) 與廠商交接帳號密碼後，應立即變更帳號密碼，同時將廠商用的帳號刪除。即每項設備從廠商獲得交接後，必須更換帳號密碼。 (3) 若帳號無法刪除，則至少應立即變更密碼。
	39	通訊網路及伺服器放置處應有門禁管制；非授權人員進出應填寫進出登記，並由內部人員陪同與監督；進出登記紀錄應定期審查，如有異常應適當處置。	§14-2	(1) 儲存個人資料之資訊設備應置放於實體安全區域(如：門禁控管之辦公區域、機房)，避免有心人士或非授權人員存取。 (2) 機房作業管理程序及指派負責人員(即需有專人看守)，例如：機房巡查、進出管制等。 (3) 訂定機房進出登記表，以管制人員與設備之進出。 (4) 來賓與廠商人員在機房作業時，指派負責人員陪同作業。 (5) 外部單位或個人更新或維修電腦設備時，應指派專人陪同，確保安全及防止個人資料外洩。 (6) 機房進出登記表，主管人員應每週或隨時抽查，若有發現不符規定或異常應立即採取行動並通知高階主管。
	40	訂定各類設備、應用軟體系統、儲存媒體之使用、報廢及轉移作業之管理規範。	§ 13-1/ § 13-2 § 14-1/ §	(1) 各類設備財產指派人員負責保管。 (2) 訂定各類設備作業使用管理程序，例如：安裝所需軟體向誰申請? 誰核准? 誰安裝? (3) 訂定報廢管理程序，即設備報廢，需有程序將原設備的資訊完整刪除。例如：硬碟、筆電或 CD 片等報廢時要經過誰檢查? 誰核准? 誰

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明(本說明不是控制措施之標準或全部作法，僅以舉例做參考說明)
			14-2 §19-4	刪除? (4) 儲存個人資料檔案之電腦或相關設備如需報廢或移轉他用時，應確實刪除該設備上所儲存之個人資料檔案。 (5) 對使用中之軟體及程式，訂定管制程序，例如：如何申請修改?如何安裝?誰才可以執行等程序。 (6) 防範資料洩漏之建議措施： i 有客戶資料之紙張不回收直接銷毀。 ii CD/硬碟/USB 等故障時，先破壞再報廢丟棄。 iii 各類設備交接或異動時作檢查，將機密或客戶資料刪除，再交接或異動。