資訊安全業務內部控制制度
共通性作業範例

科技部

中華民國 105 年 3 月修正

目　次

序　　言

「資訊安全業務內部控制制度共通性作業範例」（以下簡稱本範例）係101年4月由原行政院研究發展考核委員會依據行政院內部控制推動及督導小組第6次委員會議決議研訂，並依據第9次委員會議決定，參考專家學者及與會委員代表所提意見修正後，分行各主管機關轉知所屬參考。

本部103年12月參考ISO/IEC 27001：2013國際標準及政府組態基準(Government Configuration Baseline)，並依行政院主計總處「內部控制制度共通性制作範例」辦理本範例研修；今配合行政院104年　月頒訂「資訊系統分級與資安防護基準作業規定」及「政府內部控制監督作業要點」，爰修正本範例。

本範例內容包括資訊安全管理制度、資訊系統分級與鑑別、資安事件通報與應變等3部分，提供各機關經辦資訊安全業務人員設計機關內部控制制度時之參考。

本範例屬參考性質，各機關可依據所屬之資訊安全等級及視業務性質，於有效控制及符合法令規定情形下，合宜彈性調整。

(機關名稱)(單位名稱)作業程序說明表

項目編號	KA01
項目名稱	資訊安全管理制度
承辦單位	資訊單位
作業程序說明	一、資訊安全管理制度 (一)建立資訊安全管理制度。 (二)實作與運作資訊安全管理制度。 (三)監視與審查資訊安全管理制度。 (四)維持與改進資訊安全管理制度。 (五)資訊安全管理制度文件化。 二、資訊安全管理系統(管理階層、資訊安全組織) (一)規劃並定義出符合組織需要之資訊安全管理系統適用範圍及自組織範圍排除之理由。 (二)規劃之資訊安全管理系統應考量組織之整體業務活動及其相關風險。 (三)資訊安全管理系統(含管理決策過程)所需之文件及紀錄，應文件化及受到適當之保護與管制。 (四)資訊安全管理系統文件與紀錄發行前，應核准其適切性。 (五)應定期檢視(至少一年一次)文件與紀錄之變更與最新修訂狀況。 (六)確保文件之保護、分發、傳送、儲存以及作廢，均依據所適用之分類程序處理。 (七)管理階層對資訊安全管理系統建立、實作、運作、監視、審查、維持與改進之承諾應於文件或記錄中顯示。 (八)組織應規劃期間執行資訊安全管理系統內部稽核，以確保符合資訊安全規範、法規等要求。 (九)組織應將規劃、施行稽核、報告結果及維持紀錄之責任要求等程序加以文件化。 (十)管理階層對於稽核結果，應確保所偵測出之不符合事項及原因均已消失，並確保所採行之措施並無不當延誤。 (十一)管理階層應依規劃的期間(至少一年一次)審查資訊安全管理系統，以確保其持續之適用、適切性及有效性。 (十二)管理階層審查之審查輸入應依照機關資訊安全要求所訂之事項進行審查。 (十三)管理階層審查之審查輸出應依照機關資訊安全要求所

訂之事項進行審查。

(十四)組織應藉由使用資訊安全政策、目標、稽核結果、監視事件之分析、矯正與預防措施以及管理階層審查，以持續改進資訊安全管理系統之有效性。

(十五)組織為避免不符合事項再次發生，應進行識別、判斷原因、矯正措施審查及記錄結果等措施，並加以文件化。

(十六)組織為消除與資訊安全管理系統要求潛在不符合的原因，並防止其發生，應進行識別、決定預防措施、審查及記錄結果等措施，並加以文件化。

(十七)組織應定義與實施量測所選擇控制措施之有效性，並使用這些量測評鑑，以產生可比較與再產生的結果。

(十八)組織應建立內部及外部溝通聯繫相關措施。

三、 風險評鑑與管理(資訊安全組織、業務及資訊單位)

(一)應鑑別適用範圍內之所有資訊資產及其擁有者。

(二)應定義風險評鑑的方法論，且該方法論應確保產出可比較與可再產生的結果。

(三)應鑑別所有資產可能遭遇之威脅。

(四)應鑑別所有資產可能之脆弱點。

(五)應鑑別所有風險擁有者。

(六)應鑑別資產可能因威脅發生而喪失機密性、完整性與可用性之衝擊。

(七)應評鑑因發生安全事件而可能對組織造成之傷害及產生之後果。

(八)應評鑑安全事件發生之可能性或機率。

(九)應評鑑所有資產可能發生之風險值。

(十)組織應確定風險接受之標準與可接受風險之等級，並確保皆由管理階層核定之。

(十一)應評鑑出所有可降低風險之控制措施。

(十二)對於需要控管之風險應依其重要性決定其處理之優先順序。

(十三)應制定風險處理計畫並根據該計畫導入控制措施以降低風險。

(十四)應有書面的風險評鑑方法論、風險評鑑報告及風險處理計畫。

(十五)應定期進行風險再評鑑(至少一年一次)。

(十六)應定期評鑑脆弱點被威脅利用的可能性(至少一年一

次)。

(十七)應評鑑出可忍受最大服務中斷時間(MTPD)、資料復原點(RPO)、系統回復時間(RTO)、資料復原(WRT)。

四、安全政策(資訊安全組織及資訊單位)

(一)組織應訂有資訊安全管理系統政策。

(二)組織之資訊安全管理系統政策文件應由管理階層核准並正式發布且轉知所有員工與相關外部人員。

(三)資訊安全管理系統政策文件應包括資訊安全之目標、範圍、實施內容、執行組織、權責分工、員工責任、事件通報處理流程及違反安全政策的後果等。

(四)應指定專人或專責單位進行資訊安全管理系統政策維護及檢討。

(五)組織應定期(至少一年一次)或有重大變更時對資訊安全管理系統政策、目標之適切性及有效性，定期作必要之審查及調整。

(六)資訊安全政策應由管理階層定期進行審查(至少一年一次)。

五、資訊安全組織(資訊安全組織、人事及資訊單位)

(一)指派適當權責之高階主管負責資訊安全管理系統之協調、推動及督導等事項。

(二)成立跨部門之資訊安全推行組織負責推動、協調監督及審查資訊全管理事項。

(三)指定專人或專責單位，辦理資安政策、計畫、措施之研議，資料、資訊系統之使用管理及保護，資安認知、教育、訓練及資安稽核等資安工作事項。

(四)依一般使用者、系統管理者、系統擁有者等不同職務分別訂定其安全責任。

(五)訂定規範員工的資安作業程序與權責(含經管使用設備及作業須知)。

(六)訂定各項資訊設備的安全作業程序及授權處理層級。

(七)重要資訊處理人員應簽署保密協議並定期審查(至少一年一次)。

(八)應與相關單位如主管機關、資訊服務廠商、檢警單位、電力單位、電信單位及防救災單位建立聯絡管道。

(九)應與外界資安專家學者、資安團體或業者保持聯繫，便於取得資安技術、產品或程序等資訊。

(十)應定期(至少一年一次)或於資安作業環境發生重大變更時，召開管理審查會議，獨立審查資訊安全政策、目標、程序及控制措施。

(十一)單位內因業務需要開放給外部使用者(含其他機關、往來業者、維護廠商、委外承包商、臨僱人員及一般民眾)之資訊，應作風險鑑別，並於契約或規定中包含資料保護、資訊保密、服務水準、智慧財產權、事故發生處理及違反處理等條款。

(十二)對於開放給客戶存取權限前，應作風險評估及實施必要管控。

(十三)委外契約中應包含法律需求(如電腦處理個人資料保護法)、界定雙方有關人員權責、使用安全控管措施及作業程序、對委外廠商資安稽核權等條文。

六、 資產管理(資訊及總務單位)

(一)應鑑別資訊資產並製作資產清冊，清冊內容應隨資產異動進行更新。

(二)各項資訊資產應確定明確的擁有者、管理者及使用者。

(三)定義資訊與資產(含電子郵件、網路使用及行動設備等)之可接受使用規則。

(四)應訂有資訊分級(區分機密性、敏感性及一般性)標示與處理之相關規範。

(五)資訊應予以分級並制定標示與處置的管理程序。

七、 人力資源安全(人事、資訊及業務單位)

(一)員工應盡之安全責任應納入其工作說明書或系統文件。

(二)對人員之進用及調派，應作適當之安全評估。

(三)員工及第三方使用者應簽署保密協議並確知保密事項。

(四)對於可存取機密性、敏感性資訊或系統之員工以及配賦系統存取特別權限之員工，應有妥適分工與分散權責。

(五)管理階層應要求員工、承包商及第三方使用者，應實施組織制訂的政策及程序。

(六)員工應瞭解單位資訊安全政策及應負之資安責任。

(七)員工(含第三方使用者)應依職務層級進行適當的資訊安全認知教育與訓練。

(八)應訂有員工辦理或違反組織安全政策與程序獎懲規定。

(九)針對人員(含第三方使用者)之調動、離職或退休，應立即取消或調整其識別碼、通行碼、存取權限及安全責任。

(十)員工離職或第三方使用者於聘雇終止時，應依規定繳回其使用或保管之資訊資產並移除其存取權限。

八、實體與環境安全(資訊及稽核單位)

(一)界定重要實體區域並施予安全保護。

(二)人員進入重要實體區域應實施安全控制措施。

(三)重要實體區域的進出權限應定期審查並更新(至少一年一次)。

(四)第三方支援服務人員進入重要實體區域應經過授權並監視其活動。

(五)電腦機房及重要地區，對於進出人員應作必要之限制及監督其活動。

(六)安全區域應與易燃物或危險物品保持安全距離。

(七)電腦機房操作人員應隨時注意環境監控系統，掌握機房溫度及溼度狀況。

(八)電腦機房操作人員應熟悉自動滅火系統操作方法及滅火器位置。

(九)各項安全設備應定期檢查(至少一年一次)，員工應施予適當的安全設備使用訓練。

(十)辦公處所應實施必要之保護措施。

(十一)備援設備及備份媒體存放位置應與重要實體區域保持安全距離。

(十二)重要資訊處理設施應與一般收發或裝卸區作實體隔離。

(十三)重要資訊處理設施應特別保護並評估其有效性。

(十四)重要資訊設備之設置地點應檢查及評估火、煙、水、震動、化學效應、電力供應、電磁幅射或民間暴動等可能對設備之危害。

(十五)電源之供應及備援電源應作安全上考量。

(十六)通訊線路及電纜線應作安全保護措施。

(十七)電源線與通訊纜線應分隔，以防止互相干擾。

(十八)設備應定期維護保養(至少一年一次)，以確保其可用性及完整性。

(十九)設備送場外維修，對於儲存資訊應訂有安全保護措施。

(二十)在組織外使用資訊設備或存取資料應訂有安全保護措施。

(二十一)可攜式的電腦設備應訂有嚴謹的保護措施(如使用授權管理、設通行碼、檔案加密、專人看管)。

(二十二)設備報廢前應將機密性、敏感性資料及授權軟體予以移除或實施安全性覆寫。

(二十三)設備報廢後如確定不再使用時，應將儲存之資料及軟體移除後並做實體破壞。

(二十四)資訊資產如須攜出場外使用，應均經事前授權，並作安全查核。

(二十五)公文及儲存媒體在不使用或不在班時應妥為存放，機密性、敏感性資訊應妥為收存。

九、密碼管理(資訊及業務單位)

(一)應要求使用者對其個人通行碼盡保護及保密責任。

(二)應強制要求使用者初次登入電腦系統後必須立即更改預設之通行碼。

(三)對於忘記通行碼之處理，應要求須作身份確認程序。

(四)預設之通行碼應以安全之程序轉交於使用者，使用者取得通行碼確認無誤後需回應系統管理者。

(五)軟體安裝完畢後應立即更新廠商所預設之通行碼。

(六)使用者存取權限應定期檢查(建議每 60 天一次)或權限變更後立即複檢。

(七)通行碼應規定最小使用長度(建議 12 個字元或以上)。

(八)通行碼應規定需有大小寫字母、數字及特殊符號組成。

(九)通行碼輸入錯誤，應訂有 5 次以下之限制。

(十)應依規定期限或使用次數限制，要求變更通行碼。

(十一)應規定避免使用與個人有關資料(如生日、身份證字號、單位簡稱、電話號碼等)當作通行碼。

(十二)應用系統應具有作業結束後或在一定期間(建議 15 分鐘)未操作時即自動登出之保護機制。

(十三)對於無人看管之資訊設施應有適當保護措施。

(十四)個人電腦及終端機不使用時應關機或登出或設定螢幕通行碼或其他控制措施進行保護。

十、通訊管理(資訊及業務單位)

(一)對於資訊及軟體交換應訂有適當之交換政策、程序及控制措施。

(二)重要電腦資料媒體(含報表)之運送，應有安全保護措施並留有完整監控記錄(含收送人、時間及內容)。

(三)與外部單位間資訊與軟體之交換，應訂有交換協議。

(四)採行電子交換之資料應視資料安全等級採行識別碼通行

碼管制、電子資料加密或電子簽章認證等保護措施。

(五)對於線上交易或申辦的資訊，應訂有控制措施，以確保資訊之機密性及完整性。

(六)對外開放之資訊，應訂有保護措施以確保資訊完整性。

(七)對於採用語音、傳真及視訊通訊等設施進行資訊交換，應訂有保護控制措施。

(八)各項作業日誌應定期稽查(至少一年一次)。

(九)是否建立各項監控系統之使用程序並定期審查監控(至少一年一次)。

(十)各項日誌應有適當的保護措施。

(十一)應留有詳細的管理者與操作員之作業日誌。

(十二)資安事件日誌之記錄內容應包括使用者識別碼、登入登出之日期時間、電腦的識別資料或其網址、事件描述及矯正措施等事項。

(十三)所有系統鐘訊應定期核對校正，以確保時間記錄正確。

十一、作業管理(資訊及業務單位)

(一)資訊處理設備，應訂有書面的操作程序及管理責任。

(二)建立資訊設備與系統之變更管理程序。

(三)對安全要求高的資訊業務應將資訊安全管理及執行的職務與責任予以區隔。

(四)業務系統之使用、資料建檔、系統操作、網路管理、行政管理、系統發展維護、變更管理、安全管理等工作應授權分由不同的人員執行。

(五)開發測試系統及正常作業應區隔在不同之作業環境。

(六)建立新系統或系統升級之驗收程序(含驗收標準及應有之測試)。

(七)電腦設備設置前應進行容量規劃並預留安全容量。

(八)全面使用防毒軟體並即時更新病毒碼。

(九)定期對電腦系統及資料儲存媒體進行病毒掃描(至少一年一次)。

(十)訂定電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)。

(十一)行動碼的安裝應作必要之授權處理或限制使用。

(十二)重要的資料及軟體應定期作備份處理 (至少一年一次) 。

(十三)重要資料的備份應保留三代以上。

(十四)備份資料應異地存放，存放處所環境應合於等級之實體保護環境。

(十五)備份資料應定期回復測試(至少一年一次)，以確保備份資料之有效性。

(十六)復原程序應定期檢查與測試(至少一年一次)。

(十七)訂有電腦網路服務安全控制措施並定期檢討(至少一年一次)。

(十八)訂定安全控制措施服務水準協議(含內部或外包)之服務定義、交付等級及管理要求。

(十九)依據所訂定之服務水準協議定期監視與審查第三方的執行狀況(至少一年一次)。

(二十)網路防火牆應符合組織需要之設定。

(二十一)應定期與適時檢測網路運作環境之安全漏洞(至少一年一次)。

(二十二)對於敏感性、機密性資訊之傳送應採取資料加密等保護措施。

(二十三)應訂定可攜式媒體(磁帶、磁片、光碟片、隨身碟及報表等)管理程序。

(二十四)具機密性或敏感性資訊之媒體應有安全之保存和報廢程序。

(二十五)機密性、敏感性資料之儲存或處理應有安全處理程序及分級標示。

(二十六)系統文件應有適當之存取保護措施。

十二、存取控制(資訊及業務單位)

(一)應訂有資訊存取控制政策及相關說明文件。

(二)應訂定使用者存取權限註冊及註銷之作業程序。

(三)應定期審查並移除久未使用之使用者權限(至少一年一次)。

(四)基於系統管理或特殊作業需要，如需設定特殊權限時，應訂有嚴格管理控制措施。

(五)應訂有重要資訊不得閒置於桌面及螢幕淨空政策。

(六)網路使用者(含外單位人員)應取得正式存取授權。

(七)訂定網路服務的使用政策。

(八)對於外部連線使用者應進行鑑別機制，如密碼技術、硬體符記或詰問/應答(Challenge/Response)協定等安全技術。

(九)無線網路之存取及應用，應訂有額外的鑑別控制措施。

(十)對於遠端使用者的存取控制，應有適當的鑑別機制。
(十一)應使用自動識別設備，以鑑別來自特定地點或設備之連線。
(十二)如需採用遠端診斷作業方式，應訂定診斷埠的存取作業規範(如用金鑰管理及人員身份查驗或稽核等機制)。
(十三)依網路服務需要區隔出獨立的邏輯網域(如組織內部網路或外部網路)，每個網域皆有既定的防護措施並有通訊閘道管制過濾網域間資料的存取(如網路防火牆)。
(十四)針對電子郵件、單雙向檔案傳輸、互動式存取與存取時段作必要之安全控制措施。
(十五)應設有檢測連線的來源位址與目的位址網路路由之控管措施。
(十六)登入程序，應避免提供輔助訊息(含登入失敗訊息)。
(十七)應限制登入失敗次數的上限(建議三次)並中斷連線。
(十八)應限制登入失敗次數超過上限時需強制延遲一段時間或重新取得授權後才可再登入。
(十九)對於異常登入程序，應留有紀錄，並有專人定期檢視(至少一年一次)。
(二十)應於登入作業完成後顯示前一次登入的日期與時間，或提供登入失敗的詳細資料。
(二十一)使用者應均有唯一的識別碼。
(二十二)重要系統使用者除採一般識別碼外，應採適切的身份鑑別技術。
(二十三)通行碼應避免以網路且明文方式告知申請者。
(二十四)使用系統公用程式應作授權管制及身份鑑別程序。
(二十五)應限制網路會談結束或在一定期間未操作電腦設備時，即予中斷連線或關閉設備。
(二十六)對風險高的應用系統應限制其連線作業需求。
(二十七)對風險高的應用系統應設定連線時間限制。
(二十八)應訂有使用者及應用系統對資訊存取之權限管制措施。
(二十九)機密及敏感性資料的處理應採用專屬(隔離)的電腦作業環境。
(三十)系統存取及特別權限的配置使用情形應予以監控。
(三十一)訂定行動式電腦設備之管理政策(如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求)。

(三十二)遠距工作應得到管理階層授權和施以必要之保護措施。

十三、供應商管理(資訊及業務單位)

(一)資訊業務委外辦理時，應與廠商簽訂適當的資訊安全協定並文件化，內容是否包含資訊與通訊技術供應鏈，賦與相關的安全管理責任，並納入契約條款。

(二)資訊業務委外辦理期間，應定期對廠商所提供之服務、報告及記錄等進行監控與審查，並定期進行稽核(至少一年二次)。

(三)委外服務如有異動時，應評估資安措施之有效性，並作必要之調整。

十四、資訊系統獲取、開發及維護(資訊單位)

(一)應用系統在規劃需求時應將安全要求納入分析及規格。

(二)輸入資料應作檢查，以確認其正確且適切性。

(三)應用程式內部處理應加入檢查措施。

(四)應用系統應使用密碼技術，以鑑別與保護訊息的完整性。

(五)輸出資料應具檢查確認功能。

(六)高敏感性的資料在傳輸或儲存中應使用加密技術。

(七)密碼金鑰管理應有作業標準或管理程序。

(八)作業系統軟體更新應經管理階層授權之人員處理。

(九)作業系統升級前應作變更營運要求及版本安全性評估。

(十)測試作業應避免以真實資料進行。

(十一)原始程式庫之存取控制，應訂有控制措施。

(十二)原始程式庫之存取行為，應留有稽核日誌。

(十三)建立應用系統之變更管制程序。

(十四)系統變更後應立即更新系統文件。

(十五)作業系統變更後，應對應用系統作技術性審查。

(十六)系統變更後其相關控管措施與程序應檢查仍然有效。

(十七)系統變更後，應主動公告異動範圍、時間、可能的影響。

(十八)委外開發之系統上線前應偵測有無惡意程式。

(十九)系統安裝後應管制程式碼。

(二十)委外開發合約中應對著作權之歸屬訂有規範。

(二十一)訂約時應簽訂安全履行條款與相關罰則。

(二十二)應定期執行各項系統漏洞修補程式(至少每季一次)。

(二十三)進行系統修補前應先作系統影響評估與測試，如風險評估後，再採取必要措施。

十五、資訊安全事故管理(資訊安全組織、資訊及業務單位)

(一)建立資安事件(含安全漏洞、系統弱點、病毒、非法入侵及系統異常)之通報及處理程序。

(二)系統或服務之安全弱點，應通報至所有員工、承包商及第三方使用者。

(三)建立資安事故管理責任及應變程序。

(四)建立資安事故管理機制，如記錄事故型式、處置方法、處理成本及矯正預防措施。

(五)機關員工及外部使用者應知悉資安事件通報及處理程序並依規定辦理。

(六)資安事件中相關證據資料應有適當保護措施，以作為問題分析及法律必要依據。

(七)建立及使用有效性量測指標，以協助偵測安全事件，並預防安全事故。

十六、營運持續管理(資訊安全組織、資訊及業務單位)

(一)擬訂關鍵性業務營運衝擊分析表(BIA)。

(二)鑑別可能造成營運中斷事件之衝擊及機率，並進行風險評鑑。

(三)擬訂營運持續計畫(含啓動條件、參與人員、緊急程序、備援程序、重置程序、維護時間表、教育訓練、職責說明、所需資源、往來單位之應變規劃及合約適當性等)。

(四)營運持續計畫應定期完整測試、演練並予維護(至少一年一次)。

(五)營運持續計畫應配合業務、組織及人員之變更而更新。

(六)營運持續計畫是否定期審查和更新(至少一年一次)。

十七、遵循性(稽核、業務及資訊單位)

(一)軟體取得(含自行開發、委外開發、購置或租用)應依智慧財產權規定或合約要求確實辦理。

(二)組織重要紀錄(如資料庫紀錄、系統日誌、操作日誌、稽核日誌)應依安全等級加以保護儲存(如檔案加密或數位簽章)。

(三)組織中對於所經管或處理之資訊，涉有個人隱私及個人資料之保護應有妥適之保護機制。

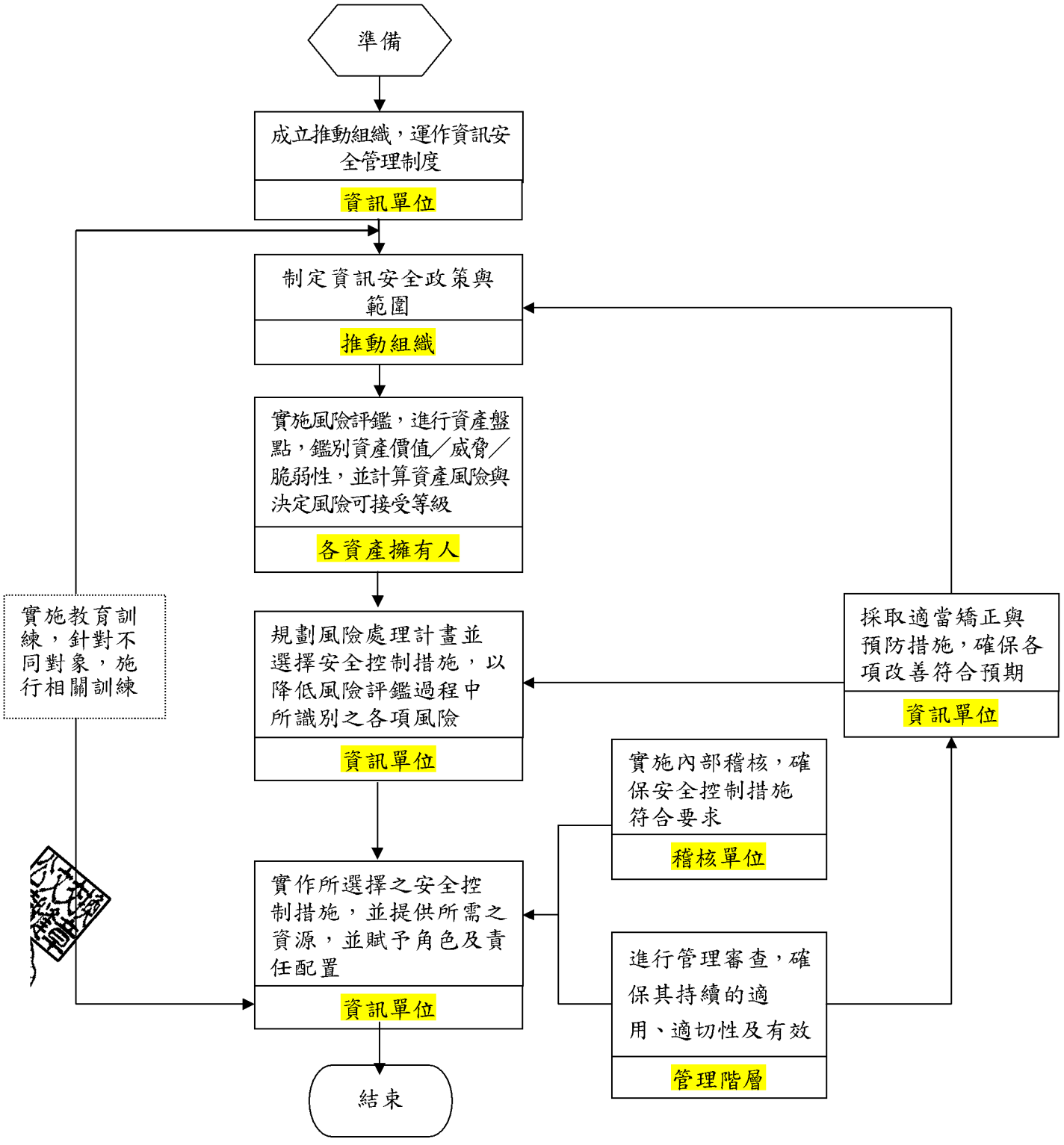
(四)應有監視設備或其他可偵測未經授權使用的設備，以防止資訊設施被不當使用。

(五)組織所訂所有安全程序，應確保相關人員能正確執行。

	(六)資訊系統應定期進行安全技術符合性的檢查(如滲透測試或系統弱點檢測)(至少一年一次)。 (七)技術符合性檢查應由合格資安技術單位或業者，經過授權的人員在其監督下或有合約規範下執行。 (八)定期辦理資訊安全內部稽核(至少一年一次)。 (九)內部稽核範圍應涵括資訊系統、供應商、資訊資產負責人、使用者和管理階層。 (十)應訂有資訊安全內部稽核計畫(含稽核目標、範圍、時間、程序、人員)。 (十一)稽核時的存取行為應作監控並留有記錄。 (十二)稽核後應產生稽核報告並追踪改善情形(包括稽核發現的摘要、稽核區域、缺失說明及改進建議等)。
控制重點	一、機關應成立資訊安全組織，以運作資訊安全管理制度。 二、機關應訂定資訊安全政策，並由管理階層核准與正式發布，且轉知所有同仁。 三、機關應實施風險評鑑，並針對評鑑結果規劃適當的風險處理計畫。 四、機關應依風險評鑑結果，針對以下之安全控制領域，實作各項安全控制措施： (一) 安全政策。 (二) 資訊安全組織。 (三) 人力資源安全。 (四) 資產管理。 (五) 存取控制。 (六) 密碼管理。 (七) 實體與環境安全。 (八) 作業管理。 (九) 通訊管理。 (十) 系統獲取、開發及維護。 (十一)供應商管理。 (十二)資訊安全事故管理。 (十三)營運持續管理。 (十四)遵循性。 五、機關應定期實施內部稽核，以確保各項安全控制措施符合要求(至少一年一次)。 六、機關之管理階層應定期審查資訊安全管理制度，以確保其

	持續的適用、適切性及有效性(至少一年一次)。 七、資訊安全管理制度中所需之文件與紀錄，應已文件化並受到適當的保護。
法令依據	一、行政院及所屬各機關資訊安全管理要點(88.09.15) 二、行政院及所屬各機關資訊安全管理規範(88.11.16)
使用表單	「資訊安全管理制度」內部控制制度控制作業層級自行評估表

「資訊安全管理制度」作業流程圖



○○機關內部控制制度控制作業層級自行評估表
○○年度

評估單位：○○

作業類別(項目)：資訊安全管理制度

評估期間：○○年○○月○○日至○○年○○月○○日　評估日期：○○年○○月○○日

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
一、作業流程有效性 (一)作業程序說明表及作業流程圖之製作是否與規定相符? (二)內部控制制度是否有效設計?						
二、資訊安全管理系統(管理階層、資訊安全組織) (一)是否已規劃並定義出符合組織需要之資訊安全管理系統之適用範圍?及自組織範圍排除之理由? (二)規劃之資訊安全管理系統是否考量組織之整體業務活動及其相關風險? (三)資訊安全管理系統(含管理決策過程)所需之文件及紀錄，是否予以文件化及受到適當之保護與管制? (四)資訊安全管理系統文件與紀錄發行前，是否核准其適切性? (五)是否定期檢視(至少一年一次)文件與紀錄的變更與最新修訂狀況? (六)是否確保文件之保護、分發、傳送、儲存以及作廢，均依據所適用的分類程序處理? (七)是否有文件或記錄顯示管理階層對資訊安全管理系統建立、實作、運作、監視、審查、維持與改進之承諾? (八)組織是否依已規劃期間執行資訊安全管理系統內部稽核，以確保符合資訊安全規範、法規等的要求? (九)組織是否將規劃、施行稽核、報告結果及維持紀錄之責任要求等程						

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
序加以文件化? (十)管理階層對於稽核結果，是否確保所偵測出之不符合事項與原因均已消失，並確保所採行的措施並無不當延誤? (十一)管理階層是否依已規劃的期間(至少一年一次)審查資訊安全管理系統，以確保其持續的適用、適切性及有效性? (十二)管理階層審查之審查輸入是否依照機關資訊安全要求所訂之事項進行審查? (十三)管理階層審查之審查輸出是否依照機關資訊安全要求所訂之事項進行審查? (十四)組織是否藉由使用資訊安全政策、目標、稽核結果、監視事件之分析、矯正與預防措施以及管理階層審查，以持續改進資訊安全管理系統之有效性? (十五)組織為避免不符合事項再次發生，是否進行識別、判斷原因、矯正措施審查及記錄結果等措施，並加以文件化? (十六)組織為消除與資訊安全管理系統要求潛在不符合的原因，並防止其發生，是否進行識別、決定預防措施、審查及記錄結果等措施，並加以文件化? (十七)組織是否定義與實施量測所選擇控制措施之有效性，並使用這些量測評鑑，以產生可比較與再產生的結果? (十八)組織是否建立內部及外部溝通聯繫相關措施?						
三、風險評鑑與管理(資訊安全組織、業務及資訊單位) (一)是否鑑別適用範圍內之所有資訊						

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
資產及其擁有者? (二)是否定義風險評鑑的方法論?該方法論並確保產出可比較與可再產生的結果? (三)是否鑑別所有資產可能遭遇之威脅? (四)是否鑑別所有資產可能之脆弱點? (五)是否鑑別風險擁有者? (六)是否鑑別資產可能因威脅發生而喪失機密性、完整性與可用性之衝擊? (七)是否評鑑因發生安全事件而可能對組織造成之傷害及產生之後果? (八)是否評鑑安全事件發生之可能性或機率? (九)是否評鑑所有資產可能發生之風險值? (十)組織是否確定風險接受之標準與可接受風險之等級?並是否皆由管理階層核定之? (十一)是否評鑑出所有可降低風險之控制措施? (十二)對於需要控管之風險是否依其重要性決定其處理之優先順序? (十三)是否制定風險處理計畫並根據該計畫導入控制措施以降低風險? (十四)是否有書面的風險評鑑方法論、風險評鑑報告及風險處理計畫? (十五)是否有定期進行風險再評鑑(至少一年一次)? (十六)是否有定期評鑑脆弱點被威脅利用的可能性(至少一年一次)?						

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
(十七)是否有評鑑出可忍受最大服務中斷時間(MTPD)、資料復原點(RPO)、系統回復時間(RTO)、資料復原(WRT)?						
四、安全政策(資訊安全組織及資訊單位) (一)組織是否訂有資訊安全管理系統政策? (二)組織之資訊安全管理系統政策文件是否由管理階層核准並正式發布且轉知所有員工與相關外部人員? (三)資訊安全管理系統政策文件是否包括資訊安全之目標、範圍、實施內容、執行組織、權責分工、員工責任、事件通報處理流程及違反安全政策的後果等? (四)是否指定專人或專責單位進行資訊安全管理系統政策維護及檢討? (五)組織是否定期(至少一年一次)或有重大變更時對資訊安全管理系統政策、目標之適切性及有效性，定期作必要之審查及調整? (六)資訊安全政策是否由管理階層每年至少審查一次?						
五、資訊安全組織(資訊安全組織、人事及資訊單位) (一)是否指派適當權責之高階主管負責資訊安全管理系統之協調、推動及督導等事項? (二)是否成立跨部門之資訊安全推行組織負責推動、協調監督及審查資訊全管理事項? (三)是否指定專人或專責單位，辦理資安政策、計畫、措施之研議，資料、資訊系統之使用管理及保護，資安認知、教育、訓練及資安稽核等資安工作事項?						

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
(四)是否依一般使用者、系統管理者、系統擁有者等不同職務分別訂定其安全責任? (五)是否訂定規範員工的資安作業程序與權責(含經管使用設備及作業須知)? (六)是否訂定各項資訊設備的安全作業程序及授權處理層級? (七)重要資訊處理人員是否簽署保密協議並定期審查(至少一年一次)? (八)是否與相關單位如主管機關、資訊服務廠商、檢警單位、電力單位、電信單位及防救災單位建立聯絡管道? (九)是否與外界資安專家學者、資安團體或業者保持聯繫，便於取得資安技術、產品或程序等資訊。 (十)是否定期(至少一年一次)或資安作業環境發生重大變更時，召開管理審查會議，獨立審查資訊安全政策、目標、程序及控制措施? (十一)單位內因業務需要開放給外部使用者(含其他機關、往來業者、維護廠商、委外承包商、臨僱人員及一般民眾)之資訊，是否作風險鑑別，並於契約或規定中包含資料保護、資訊保密、服務水準、智慧財產權、事故發生處理及違反處理等條款? (十二)對於開放給客戶存取權限前，是否作風險評估及實施必要管控? (十三)委外契約中是否包含法律需求(如電腦處理個人資料保護法)、界定雙方有關人員權責、使用安全控管措施及作業程序、對委外廠商資安稽核權等條文?						
六、資產管理(資訊及總務單位) (一)是否有資訊資產清冊，清冊內容應						

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
隨資產異動進行更新? (二)各項資訊資產是否確定明確的擁有者、管理者及使用者? (三)是否定義資訊與資產(含電子郵件、網路使用及行動設備等)之可接受使用規則? (四)是否訂有資訊分級(區分機密性、敏感性及一般性)標示與處理之相關規範? (五)資訊是否予以分級並制定標示與處置的管理程序?						
七、人力資源安全(人事、資訊及業務單位) (一)員工應盡之安全責任是否納入其工作說明書或系統文件? (二)對人員之進用及調派，是否作適當之安全評估? (三)員工及第三方使用者是否簽署保密協議並確知保密事項? (四)對於可存取機密性、敏感性資訊或系統之員工以及配賦系統存取特別權限之員工是否有妥適分工與分散權責? (五)管理階層是否有要求員工、承包商及第三方使用者，應實施組織制訂的政策及程序? (六)員工是否瞭解單位資訊安全政策及應負之資安責任? (七)員工(含第三方使用者)是否依職務層級進行適當的資訊安全認知教育與訓練? (八)是否訂有員工辦理或違反組織安全政策與程序獎懲規定? (九)針對人員(含第三方使用者)之調動、離職或退休，是否立即取消或調整其識別碼、通行碼、存取權限及安全責任?						

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
(十)員工離職或第三方使用者於聘雇終止時，是否依規定繳回其使用或保管之資訊資產並移除其存取權限?						
八、實體與環境安全(資訊及稽核單位) (一)是否界定重要實體區域並施予安全保護? (二)人員進入重要實體區域是否實施安全控制措施? (三)重要實體區域的進出權限是否定期審查並更新(至少一年一次)? (四)第三方支援服務人員進入重要實體區域是否經過授權並監視其活動? (五)電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動? (六)安全區域是否與易燃物或危險物品保持安全距離? (七)電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及溼度狀況? (八)電腦機房操作人員是否熟悉自動滅火系統操作方法及滅火器位置? (九)各項安全設備是否定期檢查(至少一年一次)?員工有否施予適當的安全設備使用訓練? (十)辦公處所是否實施必要之保護措施? (十一)備援設備及備份媒體存放位置是否與重要實體區域保持安全距離? (十二)重要資訊處理設施是否與一般收發或裝卸區作實體隔離? (十三)重要資訊處理設施是否予特別保護並評估其有效性? (十四)重要資訊設備之設置地點是否						

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
檢查及評估火、煙、水、震動、化學效應、電力供應、電磁幅射或民間暴動等可能對設備之危害? (十五)電源之供應及備援電源是否作安全上考量? (十六)通訊線路及電纜線是否作安全保護措施? (十七)電源線與通訊纜線是否分隔，以防止互相干擾? (十八)設備是否定期維護保養(至少一年一次)，以確保其可用性及完整性? (十九)設備送場外維修，對於儲存資訊是否訂有安全保護措施? (二十)在組織外使用資訊設備或存取資料是否訂有安全保護措施? (二十一)可攜式的電腦設備是否訂有嚴謹的保護措施(如使用授權管理、設通行碼、檔案加密、專人看管)? (二十二)設備報廢前是否將機密性、敏感性資料及授權軟體予以移除或實施安全性覆寫? (二十三)設備報廢後如確定不再使用時，是否將儲存之資料及軟體移除後並做實體破壞? (二十四)資訊資產如須攜出場外使用，是否均經事前授權，並作安全查核? (二十五)公文及儲存媒體在不使用或不在班時是否妥為存放?機密性、敏感性資訊是否妥為收存?						
九、密碼管理(資訊及業務單位) (一)是否要求使用者對其個人通行碼應盡保護及保密責任? (二)是否強制要求使用者初次登入電						

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
腦系統後必須立即更改預設之通行碼?						
(三)對於忘記通行碼之處理，是否要求須作身份確認程序?						
(四)預設之通行碼是否以安全之程序轉交於使用者，使用者取得通行碼確認無誤後需回應系統管理者?						
(五)軟體安裝完畢後是否立即更新廠商所預設之通行碼?						
(六)使用者存取權限是否定期檢查(建議每 60 天一次)或權限變更後立即複檢?						
(七)通行碼是否規定最小使用長度(建議 12 個字元或以上)?						
(八)通行碼是否規定需有大小寫字母、數字及特殊符號組成?						
(九)通行碼輸入錯誤，是否訂有 5 次以下之限制?						
(十)是否依規定期限或使用次數限制，要求變更通行碼?						
(十一)是否規定避免使用與個人有關資料(如生日、身份證字號、單位簡稱、電話號碼等)當作通行碼?						
(十二)應用系統是否具有作業結束後或在一定期間(建議 15 分鐘)未操作時即自動登出之保護機制?						
(十三)對於無人看管之資訊設施是否有適當保護措施?						
(十四)個人電腦及終端機不使用時是否有關機或登出或設定螢幕通行碼或其他控制措施進行保護?						
十、通訊管理(資訊及業務單位)						
(一)對於資訊及軟體交換是否訂有適當的交換政策、程序及控制措施?						
(二)重要電腦資料媒體(含報表)之運送，是否有安全保護措施並留有完整監控記錄(含收送人、時間及內						

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
容)? (三)與外部單位間資訊與軟體的交換，是否訂有交換協議? (四)採行電子交換之資料是否視資料安全等級採行識別碼通行碼管制、電子資料加密或電子簽章認證等保護措施? (五)對於線上交易或申辦的資訊，是否訂有控制措施?以確保資訊之機密性及完整性。 (六)對外開放之資訊，是否訂有保護措施以確保資訊完整性? (七)對於採用語音、傳真及視訊通訊等設施進行資訊交換，是否訂有保護控制措施? (八)各項作業日誌是否定期稽查(至少一年一次)? (九)是否建立各項監控系統之使用程序並定期審查監控(至少一年一次)? (十)各項日誌是否有適當的保護措施? (十一)是否留有詳細的管理者與操作員之作業日誌? (十二)資安事件日誌之記錄內容是否包括使用者識別碼、登入登出之日期時間、電腦的識別資料或其網址、事件描述及矯正措施等事項? (十三)所有系統鐘訊是否定期核對校正?以確保時間記錄正確。						
十一、作業管理(資訊及業務單位) (一)資訊處理設備，是否訂有書面的操作程序及管理責任? (二)是否建立資訊設備與系統之變更管理程序? (三)對安全要求高的資訊業務是否將資訊安全管理及執行的職務與責						

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
任予以區隔? (四)業務系統之使用、資料建檔、系統操作、網路管理、行政管理、系統發展維護、變更管理、安全管理等工作是否授權分由不同的人員執行? (五)開發測試系統及正常作業是否區隔在不同之作業環境? (六)是否建立新系統或系統升級之驗收程序(含驗收標準及應有之測試)? (七)電腦設備設置前是否進行容量規劃並預留安全容量? (八)是否全面使用防毒軟體並即時更新病毒碼? (九)是否定期對電腦系統及資料儲存媒體進行病毒掃描(至少一年一次)? (十)是否訂定電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)? (十一)行動碼的安裝是否作必要之授權處理或限制使用? (十二)重要的資料及軟體是否定期作備份處理(至少一年一次)? (十三)重要資料的備份是否保留三代以上? (十四)備份資料是否異地存放?存放處所環境是否合於等級之實體保護環境? (十五)備份資料是否定期回復測試(至少一年一次),以確保備份資料之有效性? (十六)復原程序是否定期檢查與測試(至少一年一次)? (十七)是否訂有電腦網路服務安全控制措施並定期檢討(至少一年一						

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
次)? (十八)是否訂定安全控制措施服務水準協議(含內部或外包)之服務定義、交付等級及管理要求? (十九)是否依據所訂定之服務水準協議定期監視與審查第三方的執行狀況(至少一年一次)? (二十)是否使用網路防火牆並作符合組織需要之設定? (二十一)是否定期與適時檢測網路運作環境之安全漏洞(至少一年一次)? (二十二)對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施? (二十三)是否訂定可攜式媒體(磁帶、磁片、光碟片、隨身碟及報表等)管理程序? (二十四)具機密性或敏感性資訊的媒體是否有安全之保存和報廢程序? (二十五)機密性、敏感性資料之儲存或處理是否有安全處理程序及分級標示? (二十六)系統文件是否有適當的存取保護措施?						
二、存取控制(資訊及業務單位) (一)是否訂有資訊存取控制政策及相關說明文件? (二)是否訂定使用者存取權限註冊及註銷之作業程序? (三)是否定期審查並移除久未使用之使用者權限(至少一年一次)? (四)基於系統管理或特殊作業需要，如需設定特殊權限時，是否訂有嚴格管理控制措施? (五)是否訂有重要資訊不得閒置於桌						

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
面及螢幕淨空政策? (六)網路使用者(含外單位人員)是否取得正式存取授權? (七)是否訂定網路服務的使用政策? (八)對於外部連線使用者是否進行鑑別機制，如密碼技術、硬體符記或詰問/應答(Challenge/Response)協定等安全技術? (九)無線網路之存取及應用，是否訂有額外的鑑別控制措施? (十)對於遠端使用者的存取控制，是否有適當的鑑別機制? (十一)是否使用自動識別設備，以鑑別來自特定地點或設備之連線? (十二)如需採用遠端診斷作業方式，是否有訂定診斷埠的存取作業規範(如用金鑰管理及人員身份查驗或稽核等機制)? (十三)是否依網路服務需要區隔出獨立的邏輯網域(如組織內部網路或外部網路)，每個網域皆有既定的防護措施並有通訊閘道管制過濾網域間資料的存取(如網路防火牆)? (十四)是否針對電子郵件、單雙向檔案傳輸、互動式存取與存取時段作必要之安全控制措施? (十五)是否設有檢測連線的來源位址與目的位址網路路由之控管措施? (十六)登入程序，是否避免提供輔助訊息(含登入失敗訊息)? (十七)是否限制登入失敗次數的上限(建議三次)並中斷連線? (十八)是否限制登入失敗次數超過上限時需強制延遲一段時間或重新取得授權後才可再登入?						

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
(十九)對於異常登入程序，是否留有紀錄，並有專人定期檢視(至少一年一次)? (二十)是否於登入作業完成後顯示前一次登入的日期與時間，或提供登入失敗的詳細資料? (二十一)使用者是否均有唯一的識別碼? (二十二)重要系統使用者除採一般識別碼外，是否採適切的身份鑑別技術? (二十三)通行碼是否避免以網路且明文方式告知申請者? (二十四)使用系統公用程式是否作授權管制及身份鑑別程序? (二十五)是否限制網路會談結束或在一定期間未操作電腦設備時,即予中斷連線或關閉設備? (二十六)對風險高的應用系統是否限制其連線作業需求? (二十七)對風險高的應用系統是否設定連線時間限制? (二十八)是否訂有使用者及應用系統對資訊存取之權限管制措施? (二十九)機密及敏感性資料的處理是否採用專屬(隔離)的電腦作業環境? (三　十)系統存取及特別權限的配置使用情形是否予以監控? (三十一)是否訂定行動式電腦設備之管理政策(如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求)? (三十二)遠距工作是否得到管理階層授權和施以必要之保護措施?						
十三、供應商管理(資訊及業務單位) (一)資訊業務委外辦理時，是否與廠商						

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
簽訂適當的資訊安全協定並文件化，內容是否包含資訊與通訊技術供應鏈，賦與相關的安全管理責任，並納入契約條款? (二)資訊業務委外辦理期間，是否定期對廠商所提供之服務、報告及記錄等進行監控與審查，並定期進行稽核(至少一年二次)? (三)委外服務如有異動時，是否評估資安措施之有效性?並作必要之調整。						
十四、資訊系統獲取、開發及維護(資訊單位) (一)應用系統在規劃需求時是否將安全要求納入分析及規格? (二)輸入資料是否作檢查，以確認其正確且適切性? (三)應用程式內部處理是否加入檢查措施? (四)應用系統是否使用密碼技術，以鑑別與保護訊息的完整性? (五)輸出資料是否具檢查確認功能? (六)高敏感性的資料在傳輸或儲存中是否使用加密技術? (七)密碼金鑰管理是否有作業標準或管理程序? (八)作業系統軟體更新是否需經管理階層授權之人員處理? (九)作業系統升級前是否作變更營運要求及版本安全性評估? (十)測試作業是否避免以真實資料進行? (十一)原始程式庫之存取控制，是否訂有控制措施? (十二)原始程式庫之存取行為，是否留有稽核日誌?						

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
(十三)是否建立應用系統之變更管制程序? (十四)系統變更後是否立即更新系統文件? (十五)作業系統變更後，是否對應用系統作技術性審查? (十六)系統變更後其相關控管措施與程序是否檢查仍然有效? (十七)系統變更後，是否主動公告異動範圍、時間、可能的影響? (十八)委外開發之系統上線前是否偵測有無惡意程式? (十九)系統安裝後是否管制程式碼? (二十)委外開發合約中是否對著作權之歸屬訂有規範? (二十一)訂約時是否簽訂安全履行條款與相關罰則? (二十二)是否定期執行各項系統漏洞修補程式(至少每季一次)? (二十三)進行系統修補前是否先作系統影響評估與測試，如風險評估後，再採取必要措施?						
十五、資訊安全事故管理(資訊安全組織、資訊及業務單位) (一)是否建立資安事件(含安全漏洞、系統弱點、病毒、非法入侵及系統異常)之通報及處理程序? (二)系統或服務之安全弱點，是否通報至所有員工、承包商及第三方使用者? (三)是否建立資安事故管理責任及應變程序? (四)是否建立資安事故管理機制，如記錄事故型式、處置方法、處理成本及矯正預防措施? (五)機關員工及外部使用者是否知悉						

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
資安事件通報及處理程序並依規定辦理? (六)資安事件中相關證據資料是否有適當保護措施?以作為問題分析及法律必要依據。 (七)是否已建立及使用有效性量測指標，以協助偵測安全事件，並預防安全事故?						
十六、營運持續管理(資訊安全組織、資訊及業務單位) (一)是否已擬訂關鍵性業務營運衝擊分析表(BIA)? (二)是否鑑別可能造成營運中斷事件之衝擊及機率，並進行風險評鑑? (三)是否擬訂營運持續計畫(含啓動條件、參與人員、緊急程序、備援程序、重置程序、維護時間表、教育訓練、職責說明、所需資源、往來單位之應變規劃及合約適當性等)? (四)營運持續計畫是否定期完整測試、演練並予維護(至少一年一次)? (五)營運持續計畫是否配合業務、組織及人員之變更而更新? (六)營運持續計畫是否定期審查和更新(至少一年一次)?						
十七、遵循性(稽核、業務及資訊單位) (一)軟體取得(含自行開發、委外開發、購置或租用)是否依智慧財產權規定或合約要求確實辦理? (二)組織重要紀錄(如資料庫紀錄、系統日誌、操作日誌、稽核日誌)是否依安全等級加以保護儲存(如檔案加密或數位簽章)? (三)組織中對於所經管或處理之資訊，涉有個人隱私及個人資料之保護是否有妥適之保護機制? (四)是否有監視設備或其他可偵測未						

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
經授權使用的設備，以防止資訊設施被不當使用? (五)組織所訂所有安全程序，是否確保相關人員能正確執行? (六)資訊系統是否定期進行安全技術符合性的檢查(如滲透測試或系統弱點檢測) (至少一年一次)? (七)技術符合性檢查是否由合格資安技術單位或業者，經過授權的人員在其監督下或有合約規範下執行? (八)是否定期辦理資訊安全內部稽核(至少一年一次)? (九)內部稽核範圍是否涵括資訊系統、供應商、資訊資產負責人、使用者和管理階層? (十)是否訂有資訊安全內部稽核計畫(含稽核目標、範圍、時間、程序、人員)? (十一)稽核時的存取行為是否作監控與並留有記錄? (十二)稽核後是否產生稽核報告並追踪改善情形(包括稽核發現的摘要、稽核區域、缺失說明及改進建議等)?						
填表人： 複核： 單位主管：						

註：

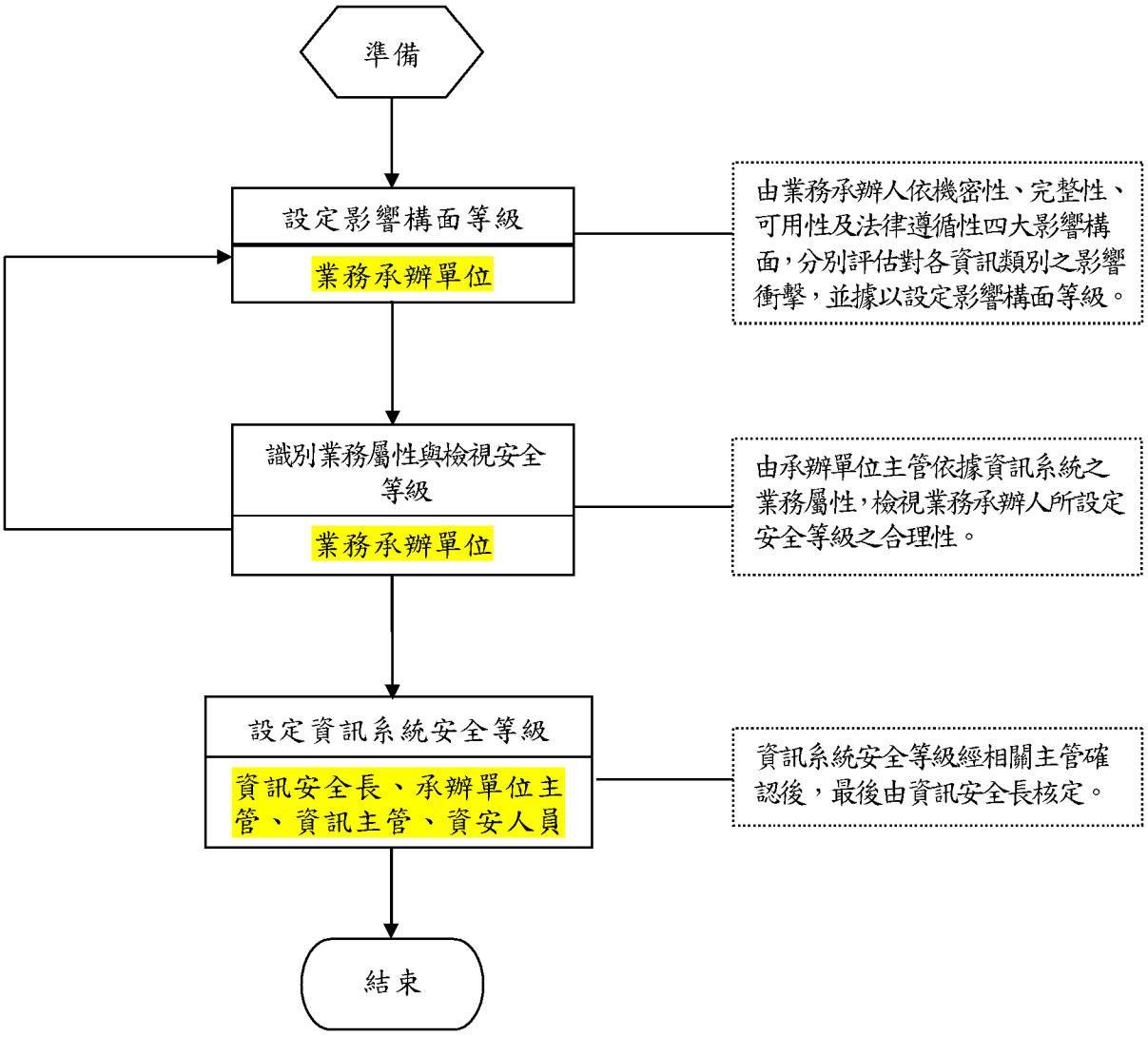
1. 機關得就1項作業流程製作1份自行評估表，亦得將各項作業流程依性質分類，同1類之作業流程合併1份自行評估表，將作業流程之控制重點納入評估。
2. 各機關依評估結果於評估情形欄勾選「落實」、「部分落實」、「未落實」、「不適用」或「其他」；其中「不適用」係指評估期間法令規定或作法已修正，但控制重點未及配合修正者；「其他」係指評估期間未發生控制重點所規範情形等，致無法評估者；遇有「部分落實」、「未落實」或「不適用」情形，於改善措施欄敘明需採行之改善措施。

(機關名稱)(單位名稱)作業程序說明表

項目編號	KA02
項目名稱	資訊系統分級與鑑別
承辦單位	資訊單位
作業程序說明	一、依據行政院國家資通安全會報訂頒之「資訊系統分級與資安防護基準作業規定」，各機關應辦理資訊系統分級與鑑別作業，以鑑別資訊系統之安全等級，掌握重點保護標的，並進行風險評鑑、有效運用資源，採行適當安全控制措施，確保資訊系統之安全防護水準。 二、資訊系統分級與鑑別作業程序如下： (一)設定影響構面等級 1.由業務承辦人評估當發生資訊安全事故時，對機密性、完整性、可用性及法律遵循性四大影響構面之衝擊程度，並參照「安全等級設定原則」(如附件 1)填寫影響構面安全等級，安全等級區分為普、中、高三級；對於不適用之影響構面，安全等級以 NA 表示。 2.資訊系統之安全等級，取其四大影響構面安全等級最高者。 (二)識別業務屬性並檢視安全等級 1.由承辦單位主管識別資訊系統之業務屬性，並與「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。 2.資訊系統依其服務之業務屬性分為行政類、業務類等二類，說明如下： (1) 行政類：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，機關得視情形調整其業務屬性。 (2) 業務類：指機關內部業務單位之業務。 3.各項異動均須記錄異動原因。 (三)設定資訊系統安全等級 1.由資訊單位綜整各項資訊系統「安全等級評估表」(如附件 2)，併同共同性系統(不需填安全等級)，彙整至「資訊系統清冊」(如附件 3)，經相關主管確認後，最後由資訊安全長核定資訊系統安全等級。 2.共同性系統包含共用性系統與共通性系統，共用性系

	統指單一機關主責系統開發與資料管理，其餘機關僅涉及使用操作。共通性系統指單一機關主責系統開發與規格制定其餘機關除使用操作外，資料主要儲存於使用機關。 3. 共同性系統之分級，統一由開發管理之機關進行評估與鑑別。 三、本作業程序所鑑別之資訊系統安全等級，可作為後續選擇安全控制措施之依據。此外，資訊系統安全等級列「高」者，可考量進一步實施詳細風險評鑑，俾利進行風險管理。
控制重點	一、機關應就四大影響構面的衝擊程度，設定資訊系統之安全等級。 二、機關應識別資訊系統之業務屬性。 三、機關應就資訊系統之業務屬性與安全等級進行勾稽。 四、機關應綜整各項資訊系統「安全等級評估表」，製作成「資訊系統清冊」，並由資訊安全長核定資訊系統安全等級。
法令依據	一、行政院及所屬各機關資訊安全管理要點(88.09.15) 二、行政院及所屬各機關資訊安全管理規範(88.11.16) 三、國家資通訊安全發展方案（102 年至 105 年）(105.02.02) 四、資訊系統分級與資安防護基準作業規定(104.07.01)
使用表單	一、「資訊系統分級與鑑別」內部控制制度控制作業層級自行評估表 二、安全等級設定原則(附件 1) 三、安全等級評估表(附件 2) 四、資訊系統清冊(附件 3)

「資訊系統分級與鑑別」作業流程圖



○○機關內部控制制度控制作業層級自行評估表
○○年度

評估單位：○○

作業類別(項目)：資訊系統分級與鑑別

評估期間：○○年○○月○○日至○○年○○月○○日　評估日期：○○年○○月○○日

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
一、作業流程有效性 (一)作業程序說明表及作業流程圖之製作是否與規定相符? (二)內部控制制度是否有效設計?						
二、是否以四大影響構面的衝擊程度，設定安全等級? 三、是否識別資訊系統之業務屬性(包括行政類、業務類等二類)? 四、是否就資訊系統之業務屬性與安全等級進行勾稽? 五、是否綜整各項資訊系統「安全等級評估表」，並製作成「資訊系統清冊」? 六、是否由資訊安全長核定資訊系統安全等級?						
填表人：　　複核：　　單位主管：						

註：

1. 機關得就1項作業流程製作1份自行評估表，亦得將各項作業流程依性質分類，同1類之作業流程合併1份自行評估表，將作業流程之控制重點納入評估。
2. 各機關依評估結果於評估情形欄勾選「落實」、「部分落實」、「未落實」、「不適用」或「其他」；其中「不適用」係指評估期間法令規定或作法已修正，但控制重點未及配合修正者；「其他」係指評估期間未發生控制重點所規範情形等，致無法評估者；遇有「部分落實」、「未落實」或「不適用」情形，於改善措施欄敘明需採行之改善措施。

附件 1　安全等級設定原則

「機密性」影響構面安全等級設定原則如下：

安全等級	說　明
普	未經授權之資訊揭露，在機關營運、資產或信譽等方面，造成可預期之有限負面影響，如： ● 一般性資料；資料外洩不致影響機關權益或僅導致機關權益輕微受損。
中	未經授權的資訊揭露，在機關營運、資產或信譽等方面，造成可預期之嚴重負面影響，如： ● 敏感性資料；資料外洩將導致機關權益嚴重受損。 ▫涉及區域性或地區性個人資料，包含出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、聯絡方式、財務情形、社會活動及其他得以直接或間接識別個人之資料。
高	未經授權之資訊揭露，在機關營運、資產或信譽等方面，造成可預期之非常嚴重或災難性負面影響，如： ● 機密性資料；資料外洩將危及國家安全、導致機關權益非常嚴重受損。 ▫凡涉及國家安全之外交、情報、國境安全、財稅、經濟、金融、醫療等重要機敏系統。 ▫特殊屬性之個人資料（如：臥底警員、受保護證人、被害人等資料），資料外洩可能會使相關個人身心受到危害、社會地位受到損害、或衍生財物損失等情形。 ▫涉及個人之醫療、基因、性生活、健康檢查、犯罪前科等資料，資料外洩將使個人權益非常嚴重受損。例如：醫療資訊系統、刑案資訊整合系統等。 ▫涉及全國性個人資料，包含出生年月日、國民身分證

安全等級	說　明
	統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、聯絡方式、財務情形、社會活動及其他得以直接或間接識別個人之資料。例如：戶役政資訊系統、護照管理系統等。

「完整性」影響構面安全等級設定原則如下：

安全等級	說　明
普	未經授權之資訊修改或破壞，在機關營運、資產或信譽等方面，造成可預期之有限負面影響，如： ● 資料遭竄改不致影響機關權益或僅導致機關權益輕微受損。
中	未經授權之資訊修改或破壞，在機關營運、資產或信譽等方面，造成可預期之嚴重負面影響，如： ● 資料遭竄改將導致機關權益嚴重受損。
高	未經授權之資訊修改或破壞，在機關、資產或信譽等方面，造成可預期之非常嚴重或災難性負面影響，如： ● 資料遭竄改將危及國家安全、導致機關權益非常嚴重受損。

「可用性」影響構面安全等級設定原則如下：

安全等級	說　明
普	資訊、資訊系統之存取或使用上的中斷，在機關營運、資產或信譽等方面，造成可預期之有限負面影響，如： ● 系統容許中斷時間較長（如：72 小時）。 ● 系統故障對社會秩序、民生體系運作不致造成影響或僅有輕微影響。 ● 系統故障造成機關業務執行效能輕微降低。

安全等級	說　明
中	資訊、資訊系統之存取或使用上的中斷，在機關營運、資產或信譽等方面，造成可預期之嚴重負面影響，如： ● 系統容許中斷時間短。 ● 系統故障對社會秩序、民生體系運作將造成嚴重影響。 ● 系統故障造成機關業務執行效能嚴重降低。
高	資訊、資訊系統之存取或使用上的中斷，在機關營運、資產或信譽等方面，造成可預期之非常嚴重或災難性負面影響，如： ● 系統容許中斷時間非常短（如：30 分鐘）。 ● 系統故障對社會秩序、民生體系運作將造成非常嚴重影響，甚至危及國家安全。 ● 系統故障造成機關業務執行效能非常嚴重降低，甚至業務停頓。

「影響法律規章遵循」影響構面安全等級設定原則如下：

安全等級	說　明
普	系統運作、資料保護、資訊資產使用等若未依循相關法律規範辦理，造成可預期之有限負面影響，如： ● **全球資訊網**：必須符合智慧財產權相關法令尊重他人智慧財產，並遵守兒童及少年福利與權益保障法進行資訊內容管理，否則將涉及違反法律之遵循性。
中	系統運作、資料保護、資訊資產使用等若未依循相關法律規範辦理，造成可預期之嚴重負面影響，如： ● **政府電子採購網**：依「政府採購法」第 27 條規定，機關辦理公開招標或選擇性招標，應將招標公告或辦理資格審查之公告刊登於政府採購公報或公開於資

安全等級	說　明
	訊網路。因此，若系統資料遭竄改導致公告資料錯誤，將影響採購作業透明化。
高	系統運作、資料保護、資訊資產使用等若未依循相關法律規範辦理，造成可預期之非常嚴重或災難性負面影響，如： ● **機密性資料**：依「國家機密保護法施行細則」第 28 條第 4 款規定，國家機密之保管方式直接儲存於資訊系統者，須將資料以政府權責主管機關認可之加密技術處理，該資訊系統並不得與外界連線。因此，機關若未依循規定儲存資料，將涉及從根本上違反法律之遵循性。 ● **醫療機構醫囑暨電子病歷系統**：依「醫療機構電子病歷製作及管理辦法」第 3 條、第 4 條規定，電子病歷資訊系統之建置、電子病歷之製作及儲存應符合相關規定。因此，機關若未依循相關規定進行系統建置維運及資料儲存，將涉及從根本上違反法律之遵循性。

附件 2　安全等級評估表

表單編號：

「OOO資訊系統」安全等級評估表

功能說明：

業務屬性：　□行政類□業務類　　日期：___年___月___日

影響構面				資訊系統安全等級
1. 機密性	2. 完整性	3. 可用性	4. 法律遵循性	
		資訊系統安全等級：		

步驟❶：設定影響構面等級

影響構面		安全等級	原因說明
1. 機密性	初估		
	異動		
2. 完整性	初估		
	異動		
3. 可用性	初估		
	異動		
4. 法律遵循性	初估		
	異動		

步驟❷：識別業務屬性

項目		業務屬性	原因說明
識別業務屬性	初估		
	異動		

備註	

承辦人	複核人員(1)	複核人員(2)	複核人員(3)	承辦單位主管

註：請各機關依本身實際陳核流程調整簽核欄位。

附件 3　資訊系統清冊

表單編號：

資訊系統清冊

彙整日期：　　年　　月　　日

編號	資訊系統名稱	業務屬性	資訊系統安全等級	共同性系統(Y/N)	承辦(管理)單位	備註
1						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						

承辦(填報)單位	審核	決行

註：請各機關依本身實際陳核流程調整簽核欄位。

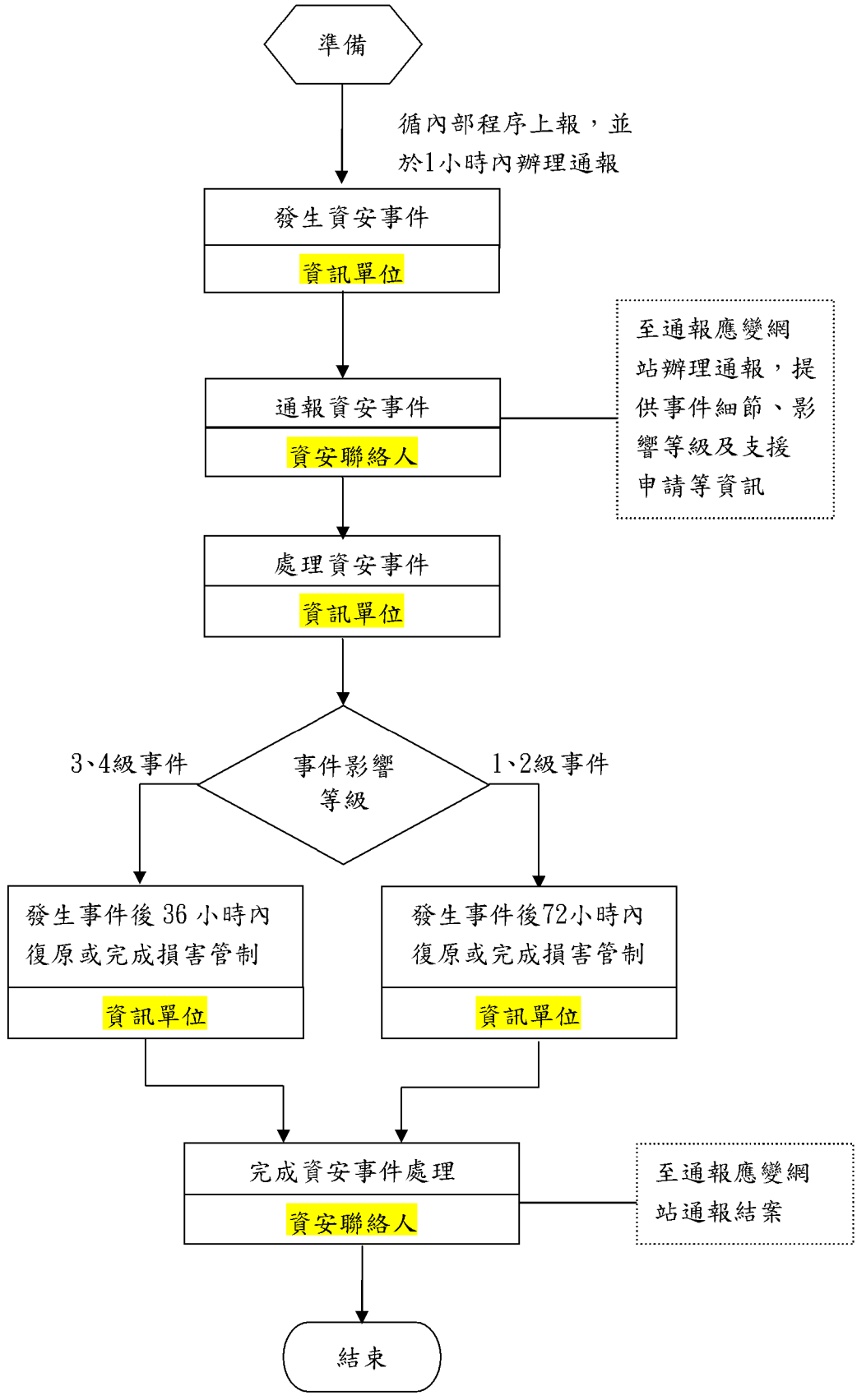
(機關名稱)(單位名稱)作業程序說明表

項目編號	KA03
項目名稱	資安事件通報與應變
承辦單位	資訊單位
作業程序說明	一、依據行政院國家資通安全會報修正之「國家資通安全通報應變綱要」，各機關應依照「資安事件通報與應變作業流程」，辦理資安事件通報與應變作業。 二、資安事件通報作業程序如下： (一) 發現資安事件後，除應循內部程序上報外，並須於 1 小時內，至「國家資通安全通報應變網站」(https://www.ncert.nat.gov.tw)通報登錄資安事件細節、影響等級及支援申請等資訊，並評估該事件是否影響其他政府機關(構)或重要民生設施運作，進行橫向通報。 (二) 如因網路或電力中斷等事由，致使無法上網填報資安事件，須於發現資安事件後 1 小時內，透過電話或傳真方式先提供事件細節，待網路通訊恢復正常後，仍須至通報應變網站補登錄通報。 (三) 進行資安事件處理，「4」、「3」級事件須於 36 小時內復原或完成損害管制；「2」、「1」級事件須於 72 小時內復原或完成損害管制。 (四) 完成資安事件處理後，須至「國家資通安全通報應變網站」通報結案，並登錄資安事件處理辦法及完成時間。 三、資安事件應變作業程序如下： (一)事前安全防護 1. 應訂定災害預防、緊急應變程序、復原計畫等防護措施並定期演練，以建立緊急應變能量。 2. 應規劃建置資通安全整體防護環境，對於機敏文件、資料及檔案等應採取加密或實體隔離等防護措施。 3. 應依資通安全防護需要，執行入侵偵測、安全掃描及弱點檢測等安全檢測工作，以做好事前防禦準備。 4. 應定期實施安全稽核、網路監控及人員安全管理等機制，以強化資通安全整體防護能力，降低安全威脅及災害損失。 5. 應針對上述建立之資通安全防護環境及相關措施，列入年度定期稽核項目，每半年實施內部稽核乙次，以

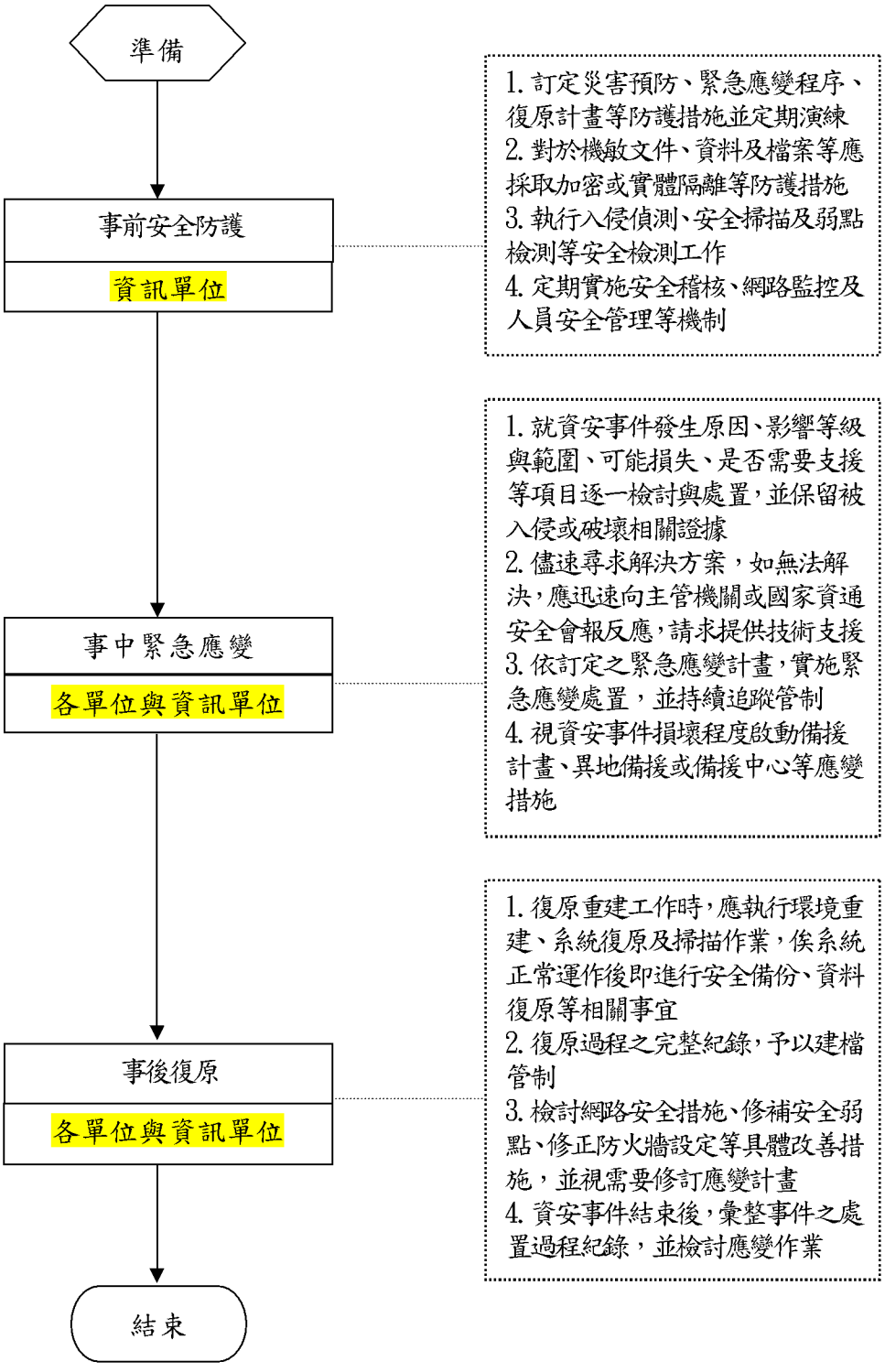
	儘早發現系統安全弱點並完成修復補強。 (二)事中緊急應變 1.應就資安事件發生原因、影響等級、可能影響範圍、可能損失、是否需要支援等項目逐一檢討與處置，並保留被入侵或破壞相關證據。 2.查詢「國家資通安全通報應變網站」、系統弱點(病毒)資料庫或聯絡技術支援單位(或廠商)等方式，尋求解決方案。如無法解決，應迅速向主管機關或國家資通安全會報反應，請求提供相關技術支援。 3.依訂定之緊急應變計畫，實施緊急應變處置，並持續監控與追蹤管制。 4.視資安事件損壞程度啟動備援計畫、異地備援或備援中心等應變措施，以防止事件擴大。 5.評估資安事件對業務運作造成之衝擊，並進行損害管制。 6.資安事件如涉及刑責，應做好證據保全工作，以聯繫檢警調單位協助偵查。 (三)事後復原作業 1.在執行復原重建工作時，應執行環境重建、系統復原及掃描作業，俟系統正常運作後即進行安全備份、資料復原等相關事宜。 2.在完成復原重建工作後，應將復原過程之完整紀錄(如資安事件原因分析及檢討改善方案、防止類似事件再次發生之具體方案、稽核軌跡及蒐集分析相關證據等資料)，予以建檔管制，以利爾後查考使用。 3.全面檢討網路安全措施、修補安全弱點、修正防火牆設定等具體改善措施，以防止類似入侵或攻擊情事再度發生，並視需要修訂應變計畫。 4.資安事件結束後，應彙整事件之處置過程紀錄、解決方案及強化措施等資訊，並提送「資通安全處理小組」檢討，以強化資通安全防護機制。
控制重點	一、機關於發生資安事件時，應依通報作業程序，於規定的期限內，至「國家資通安全通報應變網站」通報登錄資安事件

	(https://www.ncert.nat.gov.tw)。 二、機關於發生資安事件時，應於規定的期限內，進行損害管制。 三、機關應訂定災害預防、緊急應變程序、復原計畫等防護措施，並定期演練。 四、機關應針對機敏文件、資料及檔案等，採取加密或實體隔離等防護措施。 五、機關應執行入侵偵測、安全掃描及弱點檢測等安全檢測工作。 六、機關應於每半年實施內部稽核 1 次。 七、機關應於發生資安事件時，依訂定之緊急應變計畫，實施緊急應變處置。 八、機關應於資安事件結束後，彙整事件之處置過程紀錄、解決方案及強化措施等資訊，並檢討應變作業。 九、機關於資安事件處理後，應至「國家資通安全通報應變網站」通報結案。
法令依據	一、行政院及所屬各機關資訊安全管理要點(88.09.15) 二、行政院及所屬各機關資訊安全管理規範(88.11.16) 三、國家資通訊安全發展方案（102 年至 105 年）(105.02.02) 四、國家資通安全通報應變作業綱要(105.01.20)
使用表單	「資安事件通報與應變」內部控制制度控制作業層級自行評估表

「資安事件通報」作業流程圖



「資安事件應變」作業流程圖



○○機關內部控制制度控制作業層級自行評估表
○○年度

評估單位：○○

作業類別(項目)：資安事件通報與應變

評估期間：○○年○○月○○日至○○年○○月○○日　評估日期：○○年○○月○○日

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
一、作業流程有效性 (一)作業程序說明表及作業流程圖之製作是否與規定相符? (二)內部控制制度是否有效設計?						
二、發生資安事件時，是否依通報作業程序，於規定期限內，至「國家資通安全通報應變網站」通報登錄資安事件? 三、發生資安事件時，是否於規定的期限內，進行損害管制? 四、是否訂定災害預防、緊急應變程序、復原計畫等防護措施，並定期演練? 五、是否針對機敏文件、資料及檔案等採取加密或實體隔離等防護措施? 六、是否執行入侵偵測、安全掃描及弱點檢測等安全檢測工作? 七、是否於每半年實施內部稽核1次? 八、是否於發生資安事件時，依訂定之緊急應變計畫，實施緊急應變處						

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
置? 九、是否於資安事件結束後，彙整事件之處置過程紀錄、解決方案及強化措施等資訊，並檢討應變作業? 十、資安事件處理後，是否至「國家資通安全通報應變網站」通報結案?						
填表人：		複核：		單位主管：		

註：

1. 機關得就1項作業流程製作1份自行評估表，亦得將各項作業流程依性質分類，同1類之作業流程合併1份自行評估表，將作業流程之控制重點納入評估。
2. 各機關依評估結果於評估情形欄勾選「落實」、「部分落實」、「未落實」、「不適用」或「其他」；其中「不適用」係指評估期間法令規定或作法已修正，但控制重點未及配合修正者；「其他」係指評估期間未發生控制重點所規範情形等，致無法評估者；遇有「部分落實」、「未落實」或「不適用」情形，於改善措施欄敘明需採行之改善措施。