資訊系統分類分級與鑑別機制

參考手冊

行政院國家資通安全會報

中華民國 99 年 7 月

目錄

一、 依據

依據 98 年 1 月 20 日行政院函頒「國家資通訊安全發展方案（98 年至 101 年）」辦理。

二、 目的

本機制旨在鑑別資訊系統安全等級，協助機關掌握重點保護標的，並促使機關進行風險評鑑、有效運用資源，採行適當安全控制措施，以確保資訊系統之安全防護水準。

三、 適用範圍

本機制適用於各級政府機關、公營事業機構、公立研究機構、學校等（以下簡稱機關）之資訊系統，惟資訊內容屬「國家機密保護法」所稱國家機密之資訊系統，除參考本機制外，亦應依據「國家機密保護法」相關規定辦理。

四、 名詞解釋

(一) **衝擊**：故意或意外所造成不想要的事故結果。

(二) **資產**：對組織有價值的任何事物[註[1]]，包含以下形式[註[2]]：

1. **資訊**：資料庫與資料檔案、契約與協議、系統文件、操作手冊、訓練教材、研究報告、永續運作計畫、災難復原計畫、稽核紀錄及已歸檔資訊等。
2. **軟體資產**：應用軟體、系統軟體、開發工具及公用程式等。
3. **實體資產**：電腦設備、通訊設備、可移除式媒體及其他設備等。

註[1] ：資料來源為 ISO/IEC 13335-1:2004，及經濟部標準檢驗局公布國家標準 CNS 27001「資訊技術－安全技術－資訊安全管理系統－要求事項」。

註[2] ：資料來源為經濟部標準檢驗局公布國家標準 CNS 27002「資訊技術－安全技術－資訊安全管理之作業規範」。

4. **服務**：計算與通信服務、一般公用設施，例如：電源、空調、網路及照明設備等。
5. **人員**：資格、技能及經驗等。
6. **無形資產**：例如信譽及企業形象等。

(三) **資訊系統**：為協助組織決策、協調、控制、分析及實行，負責蒐集、處理、傳送、儲存及流通資訊的一組資產。[註[3]]

(四) **資訊安全**：保護資訊的機密性、完整性及可用性；此外，亦可能涉及鑑別性、可歸責性、不可否認性及可靠度等特性。[註[4]]

(五) **資訊安全事件**：系統、服務或網路相關資料顯示，可能發生資訊安全政策違例、保護措施失效、或是與安全相關而先前未知的狀況等。

(六) **資訊安全事故**：單一或一連串有顯著機率可能危害業務正常運作與威脅資訊安全的資訊安全事件。

(七) **鑑別/識別**：本參考手冊所稱「鑑別」係指依據本機制整套處理程序進行審查辨識，而「識別」係指依據本機制針對單一處理步驟進行審查辨識。

(八) **施政分類架構**：行政院為推動行政資訊種類及分類標準化，以業務功能為導向，參照資訊隸屬特性及組織執掌研訂「施政分類架構」，架構分為 19 類，包含：內政及國土安全、外交僑務及兩岸、國防及退伍軍人、財政金融、教育及體育、法務、經濟貿易、交通及建設、勞動及人力資源、農業、衛生及社會安全、環境資源、文化及觀光、國家發展及科技

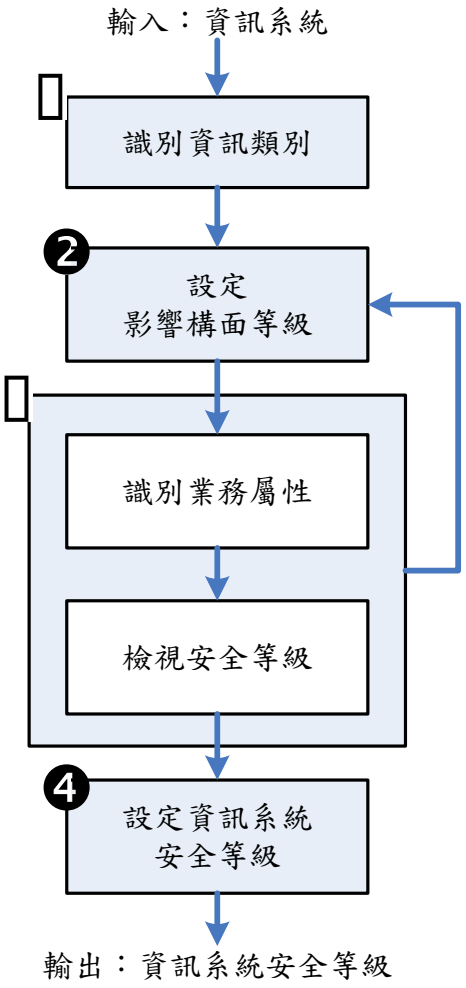
註[3]：美國 NIST SP800-60 Volume I: Guild for Mapping Type of Information and Information System to Security Categories 定義資訊系統為「負責蒐集、處理、維護、使用、分享、散播及配置資訊的一組資訊資源。」（A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.）

註[4]：資料來源為經濟部標準檢驗局公布國家標準 CNS 27002「資訊技術－安全技術－資訊安全管理之作業規範」。

、海洋事務、原住民族、客家、其他政務及輔助事務等。[註[5]]

五、 鑑別機制處理程序

本機制處理程序如圖 1 所示，包含❶識別資訊類別、❷設定影響構面等級、❸識別業務屬性並檢視安全等級、❹設定資訊系統安全等級等四個處理步驟。



❶：資訊類別即為施政分類，定義詳見行政院秘書處彙編「行政院施政分類架構」；資訊系統依其處理資料之性質，可包含多項資訊類別。

❷：由業務承辦人依資料保護受到損害、影響業務運作、影響法律規章遵循、人員傷亡、損害組織信譽及其他等六大構面，分別評估對各資訊類別之影響衝擊，並據以設定影響構面等級。

❸：由承辦單位主管依據資訊系統之業務屬性，檢視業務承辦人所設定安全等級之合理性。

❹：資訊系統安全等級經承辦單位主管、資訊主管確認後，最後由資訊安全長核定。

圖 1：資訊系統分類分級與鑑別機制處理程序

註[5]：資料來源為行政院秘書處彙編「行政院施政分類架構」。有關「施政分類架構」詳細內容請參考行政院施政分類架構知識網（http://cake.ey.gov.tw/），內文包含架構說明、分類及索引典、分類修訂原則、文件下載專區等。

各項資訊系統均須依循上述處理程序填寫「安全等級評估表」(參考範本如附件 1),並由資訊單位彙整「資訊系統清冊」(參考範本如附件 2)。為確保所鑑別安全等級符合機關安全需求,本機制依處理程序須由業務承辦人[註[6]]、承辦單位主管、資安人員、資訊主管等相關人員會辦,最後由資訊安全長核定資訊系統安全等級。機關使用附件 1、2 參考範本時,宜依機關本身實際簽核流程調整簽核欄位。

本機制主要在協助機關鑑別資訊系統安全等級、掌握重點保護標的,後續並可供機關辦理風險評鑑[註[7]]及選擇安全控制措施等,影響深遠,因此,機關每年度應針對各項資訊系統至少進行 1 次分類分級與鑑別。

另外,已通過資訊安全管理驗證(例如:ISO/IEC 27001、CNS 27001 等)機關,準用已採行之風險評鑑方法,須將資訊系統衝擊評估結果轉換為本機制之普、中、高三個安全等級。

六、 處理步驟說明

為利本機制之進行,機關於辦理資訊系統分類分級前,應先檢視本身業務性質、目標等,並進行營運衝擊分析,以資辨識核心業務[註[8]];此外,機關亦應參照「七、安全等級設定原則」,視本身業務性質,研訂符合機關業務需求之影響構面及安全等級分級準則。

有關本機制處理程序之處理步驟說明如下表,請機關相關人員依處理步驟逐項填寫「安全等級評估表」,以鑑別資訊系統安全等級。附件 4 提供共通性系統參考範例,各機關可視實際情形參考使用;另外,防毒系統、防火牆系統、入侵偵測/防禦系統

註[6]:業務承辦人係指負責該項業務之單位承辦人員,非專指資訊人員,如:戶政資訊系統之業務承辦人通常為戶政單位人員、人事系統之業務承辦人通常為人事單位人員。

註[7]:詳細內容請參考行政院研究發展考核委員會制定之「資訊系統風險評鑑參考指引」。

註[8]:詳細內容請參考行政院研究發展考核委員會「風險管理知識網」(http://www.rdec.gov.tw/mp.asp?mp=180)。

、弱點掃瞄系統、網頁/郵件內容過濾系統等屬資安防護處理相關控制措施，不需進行資訊系統分類分級與鑑別。

處理程序	工 作 項 目	相關人員
輸入： 資訊系統	● 輸入需要鑑別安全等級之資訊系統。	承辦單位主管（或其授權人員）
步驟❶： 識別資訊類別	● 「安全等級評估表」之【資訊類別】欄位係參照行政院秘書處彙編「行政院施政分類架構」之施政分類，資訊類別以取至施政分類編碼第二層為原則，惟機關可視需要自行調整至第三層或更多層。 ● 依系統涉及之業務範圍，由業務承辦人負責識別系統資訊所屬之資訊類別，並於【資訊類別】欄位以下拉式選單依次選擇資訊類別第一層、第二層編碼。	業務承辦人
步驟❷： 設定影響構面等級	● 針對所選擇之各項資訊類別，由業務承辦人評估當發生資訊安全事故時，對資料保護受到損害、影響業務運作、影響法律規章遵循、人員傷亡、損害組織信譽及其他等六大影響構面[註9]的衝擊程度，並參照「七、安全等級設定原則」填寫影響構面安全等級，安全等級區分為普、中、高三級，分別以 1、2、3 表示；對於不適用之影響構面，安全等級以 NA 表示。 ● 各項資訊類別之安全等級為該資訊類別在六大	業務承辦人

註[9]：機關發生資訊安全事故時，最容易造成的衝擊包含資料保護受到損害、影響業務運作、影響法律規章遵循、損害組織信譽、人員傷亡等五大構面；另外，考量機關不同的業務性質，可能有自行增設其他影響構面（如：財物損失）之需求。若經評估，機關可能遭遇之衝擊均已包含於前五個影響構面，則第六個影響構面得免填。

處理程序	工 作 項 目	相關人員
	影響構面安全等級最高者。因此，取各列六個影響構面安全等級值最高者即為該列【資訊類別安全等級】欄位值。 ● 資訊系統安全等級為各項資訊類別安全等級最高者。因此，取各【資訊類別安全等級】欄位值最高者即為【資訊系統安全等級】欄位值。	
步驟❸： 1. 識別業務屬性 2. 檢視安全等級	● 由承辦單位主管識別資訊系統之業務屬性，並與「步驟❷：設定影響構面等級」之結果相勾稽，以檢視所設定安全等級之合理性。 ● 資訊系統依其服務之業務屬性分為行政性業務、關鍵性業務、支援性業務等三類，說明如下： ◇ **行政性業務**：係指機關內部輔助單位[註[10]]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。 ◇ **關鍵性業務**：機關在遭遇衝擊時，須確保持續運作之核心業務，以及與民眾生活機能相關之關鍵基礎建設（如：水、電力、通訊電信、農產運銷、金融服務等），均屬關鍵性業務。 ◇ **支援性業務**：機關內部業務單位[註[11]]之業務但非列核心業務者，屬支援性業務。 ● 資訊系統安全等級與業務屬性通常具有高度關聯性，因此可進行勾稽如下： ◇ 於步驟❸-1 識別業務屬性為「行政性業務	承辦單位主管（或其授權人員）

註[10]：輔助單位包含辦理秘書、總務、人事、主計、研考、資訊、法制、政風、公關等支援服務事項之單位，詳細定義請參照中央行政機關組織基準法。

註[11]：業務單位係指執行本機關職掌事項之單位，詳細定義請參照中央行政機關組織基準法。

處理程序	工 作 項 目	相關人員
	」或「支援性業務」，惟於步驟❷設定部分資訊類別安全等級為「高」級（即等級3）。 ◇ 於步驟❸-2 識別業務屬性為「關鍵性業務」，惟於步驟❷設定各資訊類別安全等級均為「普」級（即等級1）。 如有上述情形者，機關須就其合理性進行確認，如確認無誤，則應於備註欄位說明原因。 ● 本步驟所進行各項異動均須記錄異動原因。	
步驟❹：設定資訊系統安全等級	● 由資訊單位綜整各項資訊系統「安全等級評估表」，並製作「資訊系統清冊」，經資訊主管、承辦單位主管確認後，最後由資訊安全長核定資訊系統安全等級。	資訊安全長、承辦單位主管、資訊主管、資安人員
輸出：資訊系統安全等級	● 本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[註[12]]。 ● 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[註[13]]，俾利進行風險管理。	

七、 安全等級設定原則

安全等級分為普、中、高三級，由機關依資料保護受到損害、影響業務運作、影響法律規章遵循、人員傷亡、損害組織信譽及其他等六大影響構面，分別考量資訊系統於發生資訊安全事故時可能造成的衝擊，即衡量資訊系統資料外洩、資料遭竄改、系統故障等情事時可能造成的後果嚴重程度，並據以評估、設定安全等級。

註[12]：詳細內容請參考行政院研究發展考核委員會制定之「安全控制措施參考指引」。

註[13]：詳細內容請參考行政院研究發展考核委員會制定之「資訊系統風險評鑑參考指引」。

下表安全等級設定原則可供各機關參考[註[14]]，請機關於進行本鑑別機制處理程序前，先視本身業務性質，自行調整影響構面並設定分級準則，以符合機關之業務需求。

安全等級 影響構面	普 （等級 1）	中 （等級 2）	高 （等級 3）
1. 資料保護受到損害	● 一般性資料 ● 資料若外洩或遭竄改，不致影響個人權益或僅導致個人權益輕微受損	● 敏感性資料 ● 資料若外洩或遭竄改，將導致個人權益嚴重受損	● 機密性資料 ● 資料若外洩或遭竄改，將危及國家安全、導致個人權益非常嚴重受損、或造成極大規模之個人權益嚴重受損
2. 影響業務運作	● 系統容許中斷時間較長 ● 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 ● 系統故障僅影響機關非核心業務執行效能，或造成核心業務執行效能輕微降低	● 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 ● 系統故障將造成機關核心業務執行效能嚴重降低	● 系統容許中斷時間非常短 ● 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 ● 系統故障將造成機關核心業務執行效能非常嚴重降低，甚至業務停頓
3. 影響法律規章遵循	系統運作、資料保護、資訊資產使用等須依循相關規	系統運作、資料保護、資訊資產使用等須依循相關規	系統運作、資料保護、資訊資產使用等須依循相關規

註[14]：有關各影響構面等級，另可參照行政院研究發展考核委員會「資訊系統風險評鑑參考指引」之相關輔助說明。

安全等級 影響構面	普 （等級 1）	中 （等級 2）	高 （等級 3）
	範辦理，否則將導致機關違反法律規章並伴隨輕微不良後果	範辦理，否則將導致機關違反法律規章並伴隨嚴重不良後果	範辦理，否則將導致機關從根本上違反法律規章
4. 人員傷亡	-	若系統發生資訊安全事故，無法完全排除造成人員傷亡的可能性	若系統發生資訊安全事故，可能造成人員死亡，或非常可能造成人員肢體傷害的危險
5. 損害組織信譽	若系統發生資訊安全事故，將導致機關形象、信譽受到輕微損害	若系統發生資訊安全事故，將導致機關形象、信譽受到嚴重損害	若系統發生資訊安全事故，將導致機關形象、信譽受到非常嚴重損害
6. 其他	由機關視本身業務特性考量可能遭遇衝擊之其他影響構面（如：財物損失），並依需求和本質自行設定分級基準		

資訊系統於發生資訊安全事故時，通常會同時衝擊多個影響構面。當資訊系統發生資料外洩等導致機密性喪失之情形時，可能衝擊「1.資料保護受到損害」、「3.影響法律規章遵循」、「5.損害組織信譽」等影響構面；當資訊系統發生資料遭竄改等導致完整性喪失之情形時，可能衝擊「1.資料保護受到損害」、「2.影響業務運作」、「3.影響法律規章遵循」、「4.人員傷亡」、「5.損害組織信譽」等影響構面；而當資訊系統發生系統故障等導致可用性喪失之情形時，則可能衝擊「2.影響業務運作」、「3.影響法律規章遵循」、「4.人員傷亡」、「5.損害組織信譽」等影響構面。此外，若系統發生資訊安全事故時，對於某個影響構面不造成任何危害，則該影響構面安全等級以 NA 表示不適用。

各影響構面安全等級設定原則說明如下：

(一) 影響構面「資料保護受到損害」

資訊系統發生資訊安全事故時，可能造成系統資料外洩或遭

竄改等情事，導致資料保護受到損害。因此，機關可從兩方面評估本影響構面等級：

1. **資料機密性**：應考量系統資訊之機敏性[註[15]]、涉及個人隱私程度等，評估資料外洩時可能造成的衝擊程度。
2. **資料完整性**：應考量系統資訊內容遭竄改時可能造成的衝擊程度。

「1.資料保護受到損害」影響構面安全等級設定原則如下：

安全等級	說　明
普 （等級 1）	● （資料機密性）一般性資料；資料外洩不致影響個人權益或僅導致個人權益輕微受損。 ● （資料完整性）資料遭竄改不致影響個人權益或僅導致個人權益輕微受損。
中 （等級 2）	● （資料機密性）敏感性資料；資料外洩將導致個人權益嚴重受損，如： ▫ 涉及個人出生年月日、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。 ▫ 具有敏感屬性之個人資料，如：中途輟學學生、收養兒童等資料，資料外洩可能導致個人隱私遭冒犯。 ● （資料完整性）資料遭竄改將導致個人權益嚴重受損。
高 （等級 3）	● （資料機密性）機密性資料；資料外洩將危及國家安全、導致個人權益非常嚴重受損、

註[15]：依行政院研究發展考核委員會函頒「行政院及所屬各機關資訊安全管理規範」，機關資訊安全分類可區分為機密性、敏感性及一般性等三類。

安全等級	說　明
	或造成極大規模之個人權益嚴重受損，如： ▫ 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。 ▫ 極大規模（如：全國性）之涉及個人出生年月日、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。例如：戶役政資訊系統、護照管理系統等。 ● （資料完整性）資料遭竄改將危及國家安全、導致個人權益非常嚴重受損、或造成極大規模之個人權益嚴重受損。

(二) 影響構面「影響業務運作」

資訊系統目的在輔助機關提升業務效能與服務品質，已成為機關業務運作不可或缺的一環，因此，系統故障（包含無法使用、異常運作等情形）可能導致業務執行效能降低，甚至業務中斷。

機關評估本影響構面安全等級時，應考量資訊系統可容許中斷時間、服務受影響程度等。一般而言，電子郵件系統、行政管理系統（例如：人事差勤管理系統、公文管理系統、財會系統等

）等，於系統故障時通常不致造成機關核心業務執行效能非常嚴重降低或業務中斷，因此，建議「2.影響業務運作」影響構面等級設為「普」級或「中」級。

「影響業務運作」影響構面安全等級設定原則如下：

安全等級	說　明
普 （等級 1）	● 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。 ● 系統故障僅影響機關非核心業務執行效能，或造成核心業務執行效能輕微降低。
中 （等級 2）	● 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。 ● 系統故障將造成機關核心業務執行效能嚴重降低。
高 （等級 3）	● 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。 ● 系統故障將造成機關核心業務執行效能非常嚴重降低，甚至業務停頓。

(三) 影響構面「影響法律規章遵循」

本影響構面之危害程度評估係基於機關負有遵守法律規章之責任與義務下，如發生違法情事時，機關將面臨之衝擊，本影響構面衝擊後果之嚴重程度係取決於法令規定。

政府機關依法行事，資訊使用原則上應至少符合「智慧財產權法」，資訊於網路揭露也應遵循「兒童及少年福利法」、「電腦

網路內容分級處理辦法」等。

「3.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 （等級 1）	系統運作、資料保護、資訊資產使用等須依循相關規範辦理，否則將導致機關違反法律規章並伴隨輕微不良後果，如： • **依使用授權年限購買之資訊系統或軟體：**授權年限到期，必須停止使用，否則將涉及違反契約及智慧財產權相關法令之遵循性。 • **全球資訊網：**必須符合智慧財產權相關法令尊重他人智慧結晶，並遵守兒童及少年福利法、電腦網路內容分級處理辦法進行資訊內容管理，否則將涉及違反法律之遵循性。
中 （等級 2）	系統運作、資料保護、資訊資產使用等須依循相關規範辦理，否則將導致機關違反法律規章並伴隨嚴重不良後果，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 （等級 3）	系統運作、資料保護、資訊資產使用等須依循相關規範辦理，否則將導致機關從根本上違反法律規章，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

安全等級	說　明
	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、4條規定，電子病歷資訊系統之建置、電子病歷之製作及貯存應符合相關規定。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。

(四) 影響構面「人員傷亡」

本影響構面之危害程度評估係基於直接的個人傷害，即能直接導致人身受傷、殘疾甚至死亡。機關評估本影響構面安全等級時，應考量系統故障（包含無法使用、異常運作等情形）、系統資訊遭竄改時，將危及人員生命健康之可能性及嚴重性。

「4.人員傷亡」影響構面安全等級分為兩級，設定原則如下：

安全等級	說　明
中 （等級2）	若系統發生資訊安全事故，無法完全排除造成人員傷亡的可能性。
高 （等級3）	若系統發生資訊安全事故，可能造成人員死亡，或非常可能造成人員肢體傷害的危險。

可能因發生資訊安全事故而導致人員傷亡之資訊系統，常見與飛航安全、交通安全、緊急救助、衛生醫療安全、環境安全、食品安全等相關，如：航管自動化系統、交通號誌管制系統、防救災資訊系統、緊急醫療管理系統，以及關鍵基礎建設之SCADA

（Supervisor Control And Data Acquisition）系統等，系統業務屬性通常為「關鍵性業務」。

若系統不會直接與人身安全相關（例如：人事差勤管理系統、公文管理系統、知識管理系統等），則以 NA 表示不適用。

(五) 影響構面「損害組織信譽」

資訊系統在發生資訊安全事故時，可能發生洩露機敏資料、公布錯誤資訊、核心業務停頓、關鍵基礎建設服務中斷等情形，導致損及機關之形象、信譽，甚至可能影響其他機關之形象、信譽。機關在評估本影響構面安全等級時，應考量資訊系統在機密性、完整性、可用性，或是鑑別性、可歸責性、不可否認性、可靠度等相關特性受損時，可能造成機關對外關係的負面影響程度。

「5.損害組織信譽」影響構面安全等級設定原則如下：

安全等級	說　明
普 （等級 1）	若系統發生資訊安全事故，將導致機關形象、信譽受到輕微損害，如：導致區域性媒體報導負面新聞、造成多位民眾電話抱怨等情形。
中 （等級 2）	若系統發生資訊安全事故，將導致機關形象、信譽受到嚴重損害，如：導致全國性媒體報導負面新聞、造成民眾至機關抗議或陳情等情形。
高 （等級 3）	若系統發生資訊安全事故，將導致機關形象、信譽受到非常嚴重損害，如：導致國際性媒體報導負面新聞、造成民眾大規模遊行抗爭等情形。

附件 1、安全等級評估表

表單編號：

「○○○（資訊系統名稱）」安全等級評估表

功能說明：

業務屬性：☐**關鍵性業務** ☐**支援性業務** ☐**行政性業務** **日期：**____年____月____日

編號	資訊類別（施政分類）		影響構面						資訊類別安全等級
	第一層	第二層	1. 資料保護受到損害	2. 影響業務運作	3. 影響法律規章遵循	4. 人員傷亡	5. 損害組織信譽	6. 其他(如：財物損失)	
1									
2									
3									
4									
5									
	註：資訊類別（施政分類）欄位可多選					資訊系統安全等級：			

步驟❶：識別資訊類別

項目		資訊類別	原　因　說　明
識別資訊類別（可多選）	初估		
	異動		

步驟❷：設定影響構面等級、步驟❸-2：檢視資訊類別安全等級

影響構面		安全等級	原　因　說　明
1.資料保護受到損害	初估		
	異動		
2.影響業務運作	初估		
	異動		
3.影響法律規章遵循	初估		
	異動		
4.人員傷亡	初估		
	異動		
5.損害組織信譽	初估		
	異動		
6.其他(如：財物損失)	初估		
	異動		

步驟❸-1：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，原則上，建議簽辦人員包含業務承辦人、業務單位主管、資安人員、資訊主管等。

附件 2：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	承辦單位	備註
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					

資訊單位	複核主管	資訊安全長

註：請各機關依本身實際陳核流程調整簽核欄位，如：複核主管調整為主任秘書等

附件 3：FAQ－常見問題及回答清單

(一) 資訊系統定義

Q1-1： 本文件所指「資訊系統」，與 ISO/IEC 27001 所指「資產」有何差異？

Ans： 依經濟部標準檢驗局公布 CNS 27001、CNS27002 國家標準，定義「資產（Assets）」為對組織有價值的任何事物，包含資訊、軟體資產、實體資產、服務、人員、無形資產等形式。

而本文件所指「資訊系統」係為協助組織決策、協調、控制、分析與實行，負責蒐集、處理、傳送、儲存及流通資訊的一組資產。

因此，資訊系統與資產之差異在於資訊系統是以「一組資產」呈現，例如：全球資訊網包含資訊（如：資料庫、報表、文件檔案）、軟體資產（如：應用軟體、公用程式）、實體資產（如：伺服器設備）、公用設施等資產。

Q1-2： 於資訊系統分類分級與鑑別處理程序，輸入項目為「資訊系統」，是否表示以電子檔案形式存在之敏感資訊不須進行分類分級與鑑別？

Ans： 資料檔案通常為資訊系統的一部分，而本機制是以「資訊系統」為標的，因此，機關可就具有高度關聯性的一組資產整體進行鑑別，毋須對各資產逐項進行。

若機關某業務之處理過程均以資料檔案形式為之，機關亦可對該類型資料檔案進行鑑別。

Q1-3： 資訊系統以「一組資產」呈現，導致部分具共用性質之資產（例如：資料庫）可歸屬於多個資訊系統，後續風險評鑑時，該些資產是否須重複進行多次評鑑？

Ans： 具有共用性質之資訊資產在進行後續風險評鑑時，不

須重複進行多次，但評鑑結果必須與所屬之各資訊系統安全等級進行勾稽，詳細內容可參考行政院研究發展考核委員會制訂之「資訊系統風險評鑑參考指引」。

例如：某資訊系統安全等級為「高」級，含有全國性民眾隱私資料庫，若其他安全等級為「普」級或「中」級之資訊系統，其資料庫亦安裝於前述同一資料庫主機，則宜檢視此規劃是否可能衍生資安風險。

(二) 機制之可操作性及完整性

Q2-1： 實施本機制前，需先進行哪些前置作業？

Ans： 為利實施本機制，機關於實施資訊系統分類分級前，需先進行前置作業如下：

(a) 應先瞭解機關本身特性、目標及進行營運衝擊分析等，以辨識核心業務。

(b) 應參照「七、安全等級設定原則」，視機關本身業務特質，先行研訂符合機關業務需求之影響構面及安全等級分級準則。

(c) 機關使用附件「安全防護要求等級評估表」、「資訊系統清冊」參考範本前，宜先依機關本身實際簽核流程調整簽核欄位。

(d) 實務上，機關可視需要於實施資訊系統分類分級前，先進行資訊系統盤點。

Q2-2： 本機制僅提供資訊系統分類分級與鑑別，後續機關應如何配合以提升機關防護能力？或本機制後續是否會有相關資安控制措施建議？

Ans： 資訊系統分類分級與鑑別為建立資訊安全管理之首要步驟。機關於完成資訊系統分類分級與鑑別，後續可依據所鑑別之資訊系統安全等級，參考行政院研究發展考核委員會所制定之各項資訊安全相關參考指引（

例如：資訊系統風險評鑑參考指引、安全控制措施參考指引、電子資料保護參考指引、Web 應用程式安全參考指引等)，以風險為基礎進行管理，選擇適當安全控制措施、落實執行控制措施、定期或不定期實施查核並持續改善，以強化機關資安防護能力。

Q2-3： 本機制是以六大影響構面等級最高者作為「資訊系統安全等級」，不易凸顯資訊系統之特質，是否可改以影響構面等級的比重作為計算依據，而非直接選取最大值？

Ans： 現行美、德等國家進行分類分級與鑑別，皆是先依影響構面評估安全等級，再以各影響構面等級最高者作為總體安全等級，其立論為系統若於任一構面有較高之安全防護需求，即必須以該安全等級進行整體防護，以避免不想要的事故發生。惟考量各機關業務性質不同，機關可視需要自行新增或調整影響構面，以凸顯機關特性。

Q2-4： 對於已通過 ISO/IEC 27001 或其他資訊安全管理驗證之機關雖準用已採行之風險評估方法，但若原評估結果之安全等級分為四級，而本機制卻僅分為普、中、高三級，機關應如何處理？

Ans： 已通過資訊安全管理驗證（例如：ISO/IEC 27001、CNS 27001 等）之機關，若現有風險衝擊評估並非分為三等級，機關可依據實際情形建立適當對照表，將現有等級轉化為普、中、高三級制。

參考範例：若機關現行風險評估方法依資訊資產不當存取、錯誤存取或無法存取時對機關所造成之衝擊分為四級（如下表左示），而本機制依六大影響構面之衝擊程度分為三級（如下表右示），則機關可參考兩者衝擊評估說明予以轉換如下：

現行風險評估方法（範例）			本機制	
安全等級	風險衝擊評估		衝擊評估	安全等級
1	對機關影響程度小，可忽略	→	於六大影響構面有輕微衝擊	1 (普)
2	對機關影響程度輕微			
3	對機關影響程度相當重	→	於六大影響構面有嚴重衝擊	2 (中)
4	對機關影響程度很嚴重	→	於六大影響構面有非常嚴重衝擊	3 (高)

機關原安全等級 1 之衝擊為「對機關影響程度小，可忽略」，轉換為本機制時亦可視為是輕微衝擊，因此，原等級 1、2 級可轉換為本機制之「普」級，而原等級 3、4 級則可分別轉換為本機制之「中」級、「高」級。

Q2-5： 對於已通過 ISO/IEC 27001 或其他資訊安全管理驗證之機關雖準用已採行之風險評估方法，但若原評估方式係依個別資產進行評鑑，而非以資訊系統為標的物，評估結果應如何轉化？

Ans： 機關宜先行識別資訊系統所包含資產為何，並彙整相關資產之風險評估結果，即可得出資訊系統之安全等級。

Q2-6： 依 ISO/IEC 27001 規範，風險評鑑應識別資產喪失機密性、完整性與可用性之各項衝擊，甚至須分析資產之威脅、脆弱性、發生機率等，與本機制應如何對應？

Ans： 本機制較 ISO/IEC 27001 而言相對簡易，主要係因本機制以資訊系統為評鑑標的，而非針對各項資產，且本機制利用衝擊評估資訊系統重要性，並據以要求資訊

系統最低防護水平，並不逐項分析資產之威脅、脆弱性、發生機率等。

另外，資產喪失機密性、完整性、可用性之衝擊面與本機制影響構面之對映如下：

	等級「普」	等級「中」	等級「高」
機密性	● **資料保護受到損害** ▫ 一般性資料 ▫ 資料外洩不致影響個人權益或僅導致個人權益輕微受損 ● **影響法律規章遵循** ▫ 系統運作、資料保護須依循相關規範辦理，否則將導致機關違反法律規章並伴隨輕微不良後果 ● **損害組織信譽** ▫ 資訊外洩將導致機關形象、信譽受到輕微損害	● **資料保護受到損害** ▫ 敏感性資料 ▫ 資料外洩將導致個人權益嚴重受損 ● **影響法律規章遵循** ▫ 系統運作、資料保護須依循相關規範辦理，否則將導致機關違反法律規章並伴隨嚴重不良後果 ● **損害組織信譽** ▫ 資訊外洩將導致機關形象、信譽受到嚴重損害	● **資料保護受到損害** ▫ 機密性資料 ▫ 資料外洩將危及國家安全、導致個人權益非常嚴重受損、或造成極大規模之個人權益嚴重受損 ● **影響法律規章遵循** ▫ 系統運作、資料保護須依循相關規範辦理，否則將導致機關從根本上違反法律規章 ● **損害組織信譽** ▫ 資訊外洩將導致機關形象、信譽受到非常嚴重損害
完整性	● **資料保護受到損害** ▫ 系統資料若遭竄改，不致影響個人權益或僅導致個人權益輕微受損 ● **影響業務運作** ▫ 系統資料若遭竄改，對社會秩序、民生體系運作不致造成影響或僅有輕微影響	● **資料保護受到損害** ▫ 系統資料若遭竄改，將導致個人權益嚴重受損 ● **影響業務運作** ▫ 系統資料若遭竄改，對社會秩序、民生體系運作將造成嚴重影響 ▫ 系統資料若遭竄改	● **資料保護受到損害** ▫ 系統資料若遭竄改，將危及國家安全、導致個人權益非常嚴重受損、或造成極大規模之個人權益嚴重受損 ● **影響業務運作** ▫ 系統資料若遭竄改，對社會秩序、民生體系運作將造成

	▫ 系統資料若遭竄改，僅影響機關非核心業務執行效能，或造成核心業務執行效能輕微降低 ● **影響法律規章遵循** ▫ 系統運作、資料保護須依循相關規範辦理，否則將導致機關違反法律規章並伴隨輕微不良後果 ● **損害組織信譽** ▫ 系統資料若遭竄改，將導致機關形象、信譽受到輕微損害	，將造成機關核心業務執行效能嚴重降低 ● **影響法律規章遵循** ▫ 系統運作、資料保護須依循相關規範辦理，否則將導致機關違反法律規章並伴隨嚴重不良後果 ● **人員傷亡** ▫ 系統資料若遭竄改，無法完全排除造成人員傷亡的可能性 ● **損害組織信譽** ▫ 系統資料若遭竄改，將導致機關形象、信譽受到嚴重損害	非常嚴重影響，甚至危及國家安全 ▫ 系統資料若遭竄改，將造成機關核心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** ▫ 系統運作、資料保護須依循相關規範辦理，否則將導致機關從根本上違反法律規章 ● **人員傷亡** ▫ 系統資料若遭竄改，可能造成人員死亡，或非常可能造成人員肢體傷害的危險 ● 損害組織信譽 ▫ 系統資料若遭竄改，將導致機關形象、信譽受到非常嚴重損害
可用性	● **影響業務運作** ▫ 系統容許中斷時間較長 ▫ 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 ▫ 系統故障僅影響機關非核心業務執行效能，或造成核心業務執行效能輕微	● **影響業務運作** ▫ 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 ▫ 系統故障將造成機關核心業務執行效能嚴重降低 ● **影響法律規章遵循** ▫ 資訊資產使用須依	● **影響業務運作** ▫ 系統容許中斷時間非常短 ▫ 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 ▫ 系統故障將造成機關核心業務執行效能非常嚴重降低，

	降低 ● **影響法律規章遵循** ▫ 資訊資產使用須依循相關規範辦理，否則將導致機關違反法律規章並伴隨輕微不良後果 ● **損害組織信譽** ▫ 系統故障將導致機關形象、信譽受到輕微損害	循相關規範辦理，否則將導致機關違反法律規章並伴隨嚴重不良後果 ● **人員傷亡** ▫ 系統故障無法完全排除造成人員傷亡的可能性 ● **損害組織信譽** ▫ 系統故障將導致機關形象、信譽受到嚴重損害	甚至業務停頓 ● **影響法律規章遵循** ▫ 資訊資產使用須依循相關規範辦理，否則將導致機關從根本上違反法律規章 ● **人員傷亡** ▫ 系統故障可能造成人員死亡，或非常可能造成人員肢體傷害的危險 ● **損害組織信譽** ▫ 系統故障將導致機關形象、信譽受到非常嚴重損害

(三) 業務屬性與資訊類別識別

Q3-1： 部分機關的核心業務雖配有專屬資訊系統加以輔助，然其資訊系統損毀並不會使業務實體遭致嚴重衝擊，機關應如何鑑別該類資訊系統安全等級？

Ans： 多數資訊系統之業務屬性與其安全等級具有高度關聯性，但此關聯性並非絕對。

由於機關的業務性質多樣，且資訊化、自動化程度不同，導致機關對資訊系統的依賴程度並不相同，因此，核心業務所配屬之資訊系統可能只是輔助部分核心業務運作，並非是不可中斷的。

因此，即使資訊系統經識別其服務業務屬性為關鍵性業務，資訊系統安全等級也不一定為「高」級或「中」級，亦可能為「普」級，表示系統損毀，對機關並不會造成嚴重或非常嚴重之衝擊，機關應視實際情形鑑別資訊系統安全等級。

Q3-2： 現行機關全球資訊網已成為為民服務直接且不可或缺的系統工具，一旦中斷即可能遭致民怨，或使機關信譽掃地，依業務屬性只列為行政性業務，是否可改列為關鍵性業務？

Ans： 原則上，機關全球資訊網建議歸屬為行政性業務。惟現行全球資訊網常整合多元化線上便民服務（如：即時資訊顯示、線上申辦等），機關仍宜視實際情形識別業務屬性。

另外，業務屬性與資訊系統安全等級存在高度關聯性，卻非絕對關係，即資訊系統經識別業務屬性為行政性業務，資訊系統安全等級也不一定為「普」級，亦可能為「中」級或「高」級，例如：總統府全球資訊網於我國對外形象具有象徵性意義，資訊系統安全等級即可考量列為「高」級。

Q3-3： J40 資訊類別即為「資訊」，於資訊系統分類分級與鑑別處理程序「步驟❶：識別資訊類別」，何種情形下適合選擇「J40：資訊」資訊類別？

Ans： 一般而言，系統之業務承辦單位即為資訊單位者，通常會具有「J40：資訊」資訊類別。常見系統有：全球資訊網站、電子郵件系統、目錄服務（Active Directory, AD）系統等。

Q3-4： 於資訊系統分類分級與鑑別處理程序「步驟❶：識別資訊類別」，若資訊系統（如：全球資訊網站）包含豐富且多元化資訊，應如何選擇資訊類別？

Ans： 資訊系統依其處理資料之性質，可包含多項資訊類別。然全球資訊網站包含資訊雖多，其目的主要在資訊傳播，建議歸為「J40：資訊」資訊類別即可，若網站除豐富資訊外，尚包含其他線上服務功能（例如：線上申辦、線上查詢等），則另視服務項目選擇資訊類別。

(四) 影響構面等級填寫

Q4-1： 對於主管機關或他機關所提供之資訊系統，其安全等級應如何判定？

Ans： 對於主管機關或他機關所提供之資訊系統，其安全等級宜參照原提供機關所設定之安全等級，惟機關得視機關實際應用情形調整之。

Q4-2： 如資訊系統會連結使用到其他系統儲存之資料，則應如何界定影響構面「1.資料保護受到損害」，是否須一併考量所連結使用之資料？

Ans： 對於跨系統之資料連結，應視連結使用方式考量其影響構面等級。一般而言，若資訊系統對其他系統之資料具有直接讀取能力，可能造成該資料大幅外洩情事，則識別影響構面等級時，應一併考量所連結使用之資料。舉例說明如下：

(a) 如資訊系統可直接連結其他系統之資料庫讀取資料，則識別影響構面等級時，應將所連結之資料庫視為系統之一環。

(b) 如資訊系統僅能透過 API 介面逐筆查詢其他系統儲存之資料，則該資料保護主要仍由其他資訊系統負責，識別影響構面等級時，或可不將所連結使用之資料列入考量。

Q4-3： 有關安全等級設定原則，於影響構面「3.影響法律規章遵循」，若資訊系統僅包含極少數筆個人資料，然因該些資料外洩仍會導致違反「電腦處理個人資料保護法」，是否有必要將資訊系統安全等級設為「高」級？

Ans： 有關影響構面「3.影響法律規章遵循」之安全等級評估，應考量機關違反法律規章所伴隨之後果嚴重程度作為分級基準。

若資訊系統所涉及個人資料筆數極少，且資料外洩或遭竄改不會導致個人權益非常嚴重受損，則資訊系統安全等級毋須設為「高」級。

附件 4：安全等級評估表參考範例

(一) 全球資訊網

「全球資訊網(參考範例)」安全等級評估表

功能說明：機關官方網站，提供機關簡介及政策措施介紹，並無提供線上申辦等服務。

業務屬性：☐關鍵性業務　☐支援性業務　■行政性業務　　**日期：____年____月____日**

編號	資訊類別（施政分類）		影響構面						資訊類別安全等級
	第一層	第二層	1. 資料保護受到損害	2. 影響業務運作	3. 影響法律規章遵循	4. 人員傷亡	5. 損害組織信譽	6. 其他	
1	J00 - 輔助事務	J40 - 資訊	1-普	1-普	1-普	NA	1-普[註]		1-普
2									
3									
4									
5									
								資訊系統安全等級：	1-普

註：全球資訊網所提供服務性質較為多元化，機關宜視本身實際情形評估影響構面等級。

步驟❶：識別資訊類別

項目		資訊類別	原　因　說　明
識別資訊類別	初估	J40 - 資訊	全球資訊網在提供機關對外資訊服務，J40資訊類別包含J49-政府資訊服務
	異動		

步驟❷：設定影響構面等級、步驟❸-2：檢視資訊類別安全等級

影響構面		安全等級	原　因　說　明
1.資料保護受到損害	初估	1-普	網站資訊均為可公開之一般性資料
	異動		
2.影響業務運作	初估	1-普	本網站主要提供資訊公告，系統中斷不影響核心業務
	異動		
3.影響法律規章遵循	初估	1-普	本網站必須符合智慧財產權相關法令，及遵守兒童及少年福利法、電腦網路內容分級處理辦法，惟不涉及從根本上違反法律之可能性，也不致因違反規範導致嚴重不良後果
	異動		
4.人員傷亡	初估	NA	本網站提供一般性資料瀏覽，不會直接造成人員傷亡
	異動		
5.損害組織信譽	初估	1-普	本機關非屬軍事、外交、情報等機敏機關，業務屬性亦不具高度機敏性，惟網站遭遇資訊安全事件，評估仍可能導致國內媒體報導負面新聞，但不致導致機關信譽受到嚴重或非常嚴重損害
	異動		
6.其他(如：財物損失)	初估		
	異動		

步驟❸-1：識別業務屬性

項目		業務屬性	原　因　說　明
識別業務屬性	初估	行政性業務	本案提供機關簡介、政策措施介紹等對外資訊服務，並無涉及機關業務線上申辦等其他服務，屬行政性業務
	異動		

備註	

(二) 電子郵件系統

「電子郵件系統(參考範例)」安全等級評估表

功能說明：提供機關同仁電子郵件服務。

業務屬性：☐關鍵性業務　☐支援性業務　■行政性業務　　**日期：____年____月____日**

編號	資訊類別（施政分類）		影響構面						資訊類別安全等級
	第一層	第二層	1. 資料保護受到損害	2. 影響業務運作	3. 影響法律規章遵循	4. 人員傷亡	5. 損害組織信譽	6. 其他	
1	J00 - 輔助事務	J40 - 資訊	1-普	1-普	NA	NA	1-普		1-普
2									
3									
4									
5									
								資訊系統安全等級：	1-普

步驟❶：識別資訊類別

項目		資訊類別	原　因　說　明
識別資訊類別	初估	J40 - 資訊	電子郵件系統在提供機關同仁電子郵件收發之機關內部資訊服務，屬「J40-資訊」類別
	異動		

步驟❷：設定影響構面等級、步驟❸-2：檢視資訊類別安全等級

影響構面		安全等級	原　因　說　明
1.資料保護受到損害	初估	1-普	系統包含機關同仁電子郵件帳號，惟依本機關業務性質，公務用郵件帳號屬公開資料，並不涉及機密性與敏感性
	異動		
2.影響業務運作	初估	1-普	系統服務停止將造成機關對外收發郵件服務中斷，部分業務可能受到影響，但不致造成核心業務執行效能嚴重降低
	異動		
3.影響法律規章遵循	初估	NA	本系統提供電子郵件服務，其系統運作並無直接涉及法令規範，不致導致機關違反法律規章並伴隨不良後果
	異動		
4.人員傷亡	初估	NA	本系統提供電子郵件服務，不會直接造成人員傷亡
	異動		
5.損害組織信譽	初估	1-普	本機關非屬軍車、外交、情報等機敏機關，惟如本系統遭駭而大量濫發惡意電子郵件，評估仍可能導致國內媒體報導負面新聞，但不致導致機關信譽受到嚴重或非常嚴重損害
	異動		
6.其他(如：財物損失)	初估		
	異動		

步驟❸-1：識別業務屬性

項目		業務屬性	原　因　說　明
識別業務屬性	初估	行政性業務	本案為機關內部輔助單位（資訊單位）之業務，屬行政性業務
	異動		

備註	

(三) 電子表單系統

「電子表單系統(參考範例)」安全等級評估表

功能說明：提供機關同仁線上申請出差、派車、加班、請假、文具採購等作業。

業務屬性：☐關鍵性業務 ☐支援性業務 ■行政性業務 **日期：____年____月____日**

編號	資訊類別（施政分類）		影響構面						資訊類別安全等級
	第一層	第二層	1. 資料保護受到損害	2. 影響業務運作	3. 影響法律規章遵循	4. 人員傷亡	5. 損害組織信譽	6. 其他	
1	J00 - 輔助事務	J10 - 人事	1-普	1-普	NA	NA	1-普		1-普
2	J00 - 輔助事務	J50 - 秘書總務	1-普	1-普	NA	NA	1-普		1-普
3									
4									
5									
								資訊系統安全等級：	1-普

步驟❶：識別資訊類別

項目		資訊類別	原 因 說 明
識別資訊類別	初估	J10-人事；J50-秘書總務	本系統包含出差、加班、請假等人事差勤資料，以及派車、文具採購等庶務資料
	異動		

步驟❷：設定影響構面等級、步驟❸-2：檢視資訊類別安全等級

影響構面		安全等級	原 因 說 明
1.資料保護受到損害	初估	1-普	系統資料屬一般性資料，並無敏感性個人資料或其他機密資料
	異動		
2.影響業務運作	初估	1-普	本系統容許中斷時間較長（超過24小時），且服務中斷不致影響核心業務運作
	異動		
3.影響法律規章遵循	初估	NA	本系統提供機關內部同仁線上表單申請，其系統運作並無直接涉及法令規範，不致導致機關違反法律規章並伴隨不良後果
	異動		
4.人員傷亡	初估	NA	本系統目的在提供機關同仁線上表單申請，不會直接造成人員傷亡
	異動		
5.損害組織信譽	初估	1-普	本系統不對外提供服務；另，本機關非屬軍事、外交、情報等機敏機關，評估表單申請資料外洩評估可能導致國內媒體報導負面新聞，但不致導致機關信譽受到嚴重或非常嚴重損害
	異動		
6.其他(如：財物損失)	初估		
	異動		

步驟❸-1：識別業務屬性

項目		業務屬性	原 因 說 明
識別業務屬性	初估	行政性業務	本系統目的在提供機關同仁內部表單申請，屬行政性業務
	異動		

備註	

(四) 人事管理系統

「人事管理系統(參考範例)」安全等級評估表

功能說明：提供機關同仁進行差勤線上申請，以及人事單位進行相關人事差勤管理。

業務屬性：☐關鍵性業務　☐支援性業務　■行政性業務　　**日期：____年____月____日**

編號	資訊類別（施政分類）		影響構面						資訊類別安全等級
	第一層	第二層	1. 資料保護受到損害	2. 影響業務運作	3. 影響法律規章遵循	4. 人員傷亡	5. 損害組織信譽	6. 其他	
1	J00 - 輔助事務	J10 - 人事	2-中	1-普	1-普	NA	1-普		2-中
2									
3									
4									
5									
								資訊系統安全等級：	2-中

步驟❶：識別資訊類別

項目		資訊類別	原　因　說　明
識別資訊類別	初估	J10 - 人事	人事管理系統包含機關編制、任免陞遷、差假（勤）管理、考績獎懲、俸給待遇等人事資料
	異動		

步驟❷：設定影響構面等級、步驟❸-2：檢視資訊類別安全等級

影響構面		安全等級	原　因　說　明
1.資料保護受到損害	初估	2-中	本系統包含機關同仁之身份證字號、出生年月日、戶籍地址、聯絡住址、電話、俸給待遇等人事基本資料，屬敏感性資料
	異動		
2.影響業務運作	初估	1-普	本系統容許中斷時間較長（超過24小時），且服務中斷不致影響核心業務運作
	異動		
3.影響法律規章遵循	初估	1-普	本系統包含機關同仁基本個人資料，應依「個人資料保護法」規定辦理；惟資料筆數不多，且多屬個人基本資料，評估若未完成遵循個資法辦理資料保護，可能伴隨輕微不良後果
	異動		
4.人員傷亡	初估	NA	本系統目的在提供人事管理服務，不會直接造成人員傷亡
	異動		
5.損害組織信譽	初估	1-普	本系統不對外提供服務；另，本機關非屬軍事、外交、情報等機敏機關，評估同仁名錄外洩可能導致國內媒體報導負面新聞，但不致導致機關信譽受到嚴重或非常嚴重損害
	異動		
6.其他(如：財物損失)	初估		
	異動		

步驟❸-1：識別業務屬性

項目		業務屬性	原　因　說　明
識別業務屬性	初估	行政性業務	機關內部人事管理屬行政性業務
	異動		

備註	

(五) 會計管理系統

「會計管理系統(參考範例)」安全等級評估表

功能說明：提供機關會計人員進行會計帳務作業及管理。

業務屬性：☐關鍵性業務　☐支援性業務　■行政性業務　　**日期：____年____月____日**

編號	資訊類別（施政分類）		影響構面						資訊類別安全等級
	第一層	第二層	1. 資料保護受到損害	2. 影響業務運作	3. 影響法律規章遵循	4. 人員傷亡	5. 損害組織信譽	6. 其他	
1	J00 - 輔助事務	J20 - 主計	2-中	1-普	2-中	NA	2-中		2-中
2									
3									
4									
5									
								資訊系統安全等級：	2-中

步驟❶：識別資訊類別

項目		資訊類別	原　因　說　明
識別資訊類別	初估	J20 - 主計	主計資料包含J21歲計、J22會計等資料，本系統主要為會計資料
	異動		

步驟❷：設定影響構面等級、步驟❸-2：檢視資訊類別安全等級

影響構面		安全等級	原　因　說　明
1.資料保護受到損害	初估	2-中	系統包含本機關收入、支出明細資料，屬敏感性資料
	異動		
2.影響業務運作	初估	1-普	本系統容許中斷時間較長（超過24小時），且服務中斷不致影響核心業務運作
	異動		
3.影響法律規章遵循	初估	2-中	會計系統資料包含受款人資料（包含姓名、戶籍地址、身分證字號、金融帳號等）及帳務往來明細等，應依「個人資料保護法」規定辦理
	異動		
4.人員傷亡	初估	NA	本系統目的在提供會計帳務管理，不會直接造成人員傷亡
	異動		
5.損害組織信譽	初估	2-中	本系統不對外提供服務，惟會計帳務資料屬敏感性資料，評估外洩時可能導致機關信譽受到嚴重損害
	異動		
6.其他(如：財物損失)	初估		
	異動		

步驟❸-1：識別業務屬性

項目		業務屬性	原　因　說　明
識別業務屬性	初估	行政性業務	機關內部會計管理屬行政性業務
	異動		

備註	