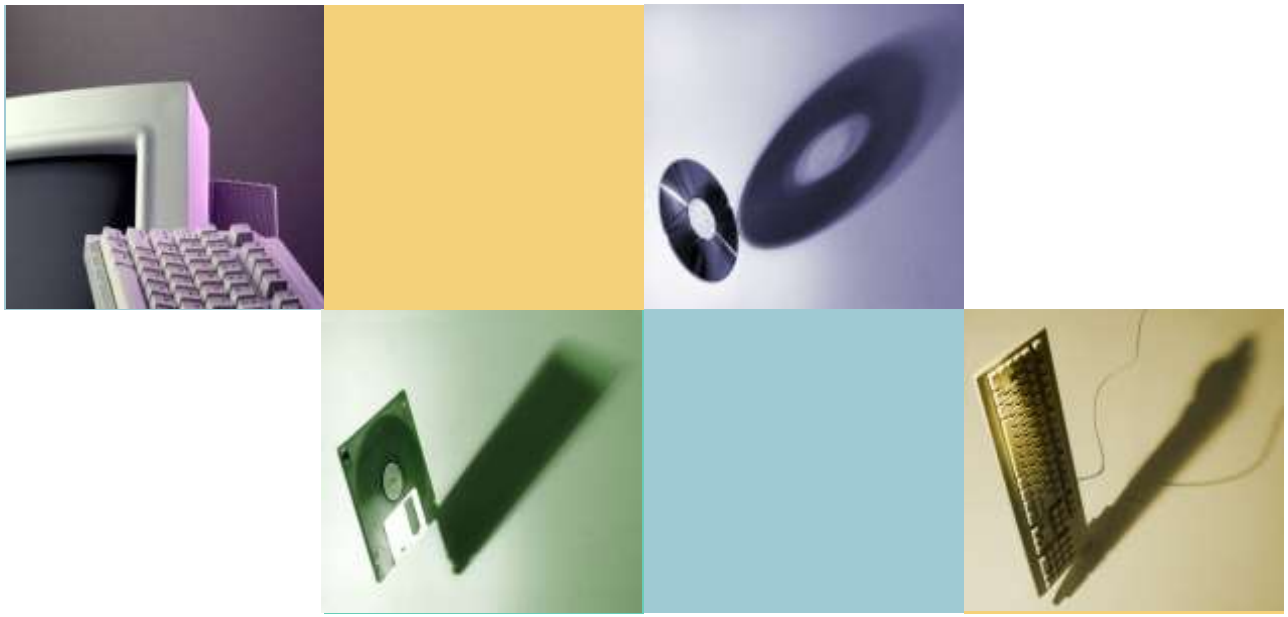
資訊系統分級與資安防護基準作業規定介紹



Wednesday, Nov 18 2015

曾國旭

目的及適用範圍

- 目的
  - 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
- 適用範圍
  - 適用於「政府機關（構）資通安全責任等級分級作業規定」應辦事項所律定對象之資訊系統
  - 教育體系依「教育部與所屬機關(構)及學校資通安全責任等級分級作業規定」



資訊系統分級作業

- 需要進行分級之資訊系統，以自行或委外開發之資訊系統為主
- 套裝軟體、作業系統或防毒系統、防火牆系統、入侵偵測/防禦系統、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，均不需進行資訊系統分級
- 分級後之資訊系統，依照所設定之安全等級，作為後續執行防護基準之依據。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



資訊系統分級步驟(1/3)

- 設定影響構面等級
  - 由業務承辦人評估當發生資安事件時，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」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 (Not Applicable)表示
  - 資訊系統之安全等級，取其四大影響構面安全等級最高者



資訊系統分級步驟(2/3)

- 識別業務屬性，檢視安全等級
  - 識別資訊系統之業務屬性，並由承辦單位主管檢視設定安全等級之合理性
  - 資訊系統依其支援之單位及業務屬性，分為行政與業務二類，說明如下：
    - 行政類： 指機關內部輔助單位之業務（如：人事、薪資等），惟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類別
    - 業務類：指機關內部業務單位之業務（如：交通監理、便民服務等）
  - 本步驟所進行各項異動均須記錄異動原因

資訊系統分級步驟(3/3)

- 核定資訊系統安全等級
  - 由資訊單位綜整各資訊系統「安全等級評估表」中資訊，併同共同性系統(不需填安全等級)，彙整至「資訊系統清冊」，資訊系統安全等級經相關主管確認後，最後由資訊安全長核定。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
  - 共同性系統包含共用性系統與共通性系統，說明如下：
    - 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，如國稅系統
    - 共通性系統指單一機關主責系統開發與規格制訂，其餘機關除使用操作外，資料主要儲存於使用機關，如公文電子交換系統

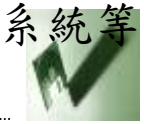
安全等級設定原則-機密性(1/7)

- 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



安全等級設定原則-機密性(2/7)

- 高：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



安全等級設定原則-完整性(3/7)

- 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



安全等級設定原則-可用性(4/7)

- 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，行政類系統（例如：人事管理系統、會計系統等）等，於系統故障時通常不致造成機關業務執行效能嚴重降低或業務中斷
- 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



安全等級設定原則-可用性(5/7)

- 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



安全等級設定原則-法律遵循性(6/7)

- 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相關法令，資訊於網路揭露也應遵循「兒童及少年福利與權益保障法」及其相關規定
- 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



安全等級設定原則-法律遵循性(7/7)

- 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

防護基準項目及控制措施(1/4)

- 存取控制(Access Control)
  - 帳號管理(Account Management)
  - 最小權限(Least Privilege)
  - 遠端存取(Remote Access)
- 稽核與可歸責性(Audit and Accountability)
  - 稽核事件(Audit Events)
  - 稽核紀錄內容(Content of Audit Records)
  - 稽核儲存容量(Audit Storage Capacity)
  - 稽核處理失效之回應(Response to Audit Processing Failures)
  - 時戳(Time Stamps)
  - 稽核資訊之保護(Protection of Audit Information)
- 營運持續計畫
  - 資訊系統備份(Information System Backup)
  - 資訊系統備援(Redundancy of Information Systems)



防護基準項目及控制措施(2/4)

- 識別與鑑別(Identification and Authentication)
  - 使用者之識別與鑑別(Identification and Authentication)
  - 裝置之識別與鑑別(Device Identification and Authentication)
  - 鑑別資訊管理(Authenticator Management)
  - 鑑別資訊回饋(Authenticator Feedback)
  - 加密模組鑑別(Cryptographic Module Authentication)
- 系統與通訊保護(System and Communications Protection)
  - 傳輸之機密性與完整性(Transmission Confidentiality and Integrity)
  - 資料儲存之安全(Protection of Information at Rest)



防護基準項目及控制措施(3/4)

- 系統與服務獲得(System and Services Acquisition)
  - 系統發展生命週期需求階段(System Development Life Cycle-Requirement)
  - 系統發展生命週期設計階段(System Development Life Cycle-Design)
  - 系統發展生命週期開發階段(System Development Life Cycle-Develop)
  - 系統發展生命週期測試階段(System Development Life Cycle-Test)
  - 系統發展生命週期部署與維運階段(System Development Life Cycle-Deployment and Maintenance)
  - 系統發展生命週期委外階段(System Development Life Cycle-Outsourcing)
  - 獲得程序(Acquisition Process)
  - 資訊系統文件(Information System Documentation)



防護基準項目及控制措施(4/4)

- 系統與通訊保護(System and Communications Protection)
  - 傳輸之機密性與完整性(Transmission Confidentiality and Integrity)
  - 資料儲存之安全(Protection of Information at Rest)
- 系統與資訊完整性(System and Information Integrity)
  - 漏洞修復(Flaw Remediation)
  - 資訊系統監控(Information System Monitoring)
  - 軟體及資訊完整性(Software, Firmware, and Information Integrity)
- 各控制措施之詳細執行說明請參考「資訊系統分級與資安防護基準作業規定」

安全等級評估表範例(1/3)

「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：□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	
普	普	普	普	普
		資訊系統安全等級：		普

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	普	網站資訊均為可公開之一般性資料
	異動		
2. 完整性	初估	普	本網站主要提供資訊公告
	異動		
3. 可用性	初估	普	本網站提供一般性資料瀏覽
	異動		
4. 法律遵循性	初估	普	本網站必須符合智慧財產權相關法令，並遵守兒童及少年福利與權益保障法及其相關規定，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		

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	業務類	本系統提供機關簡介、政策措施介紹等對外資訊服務，無涉及機關業務線上申辦等其他服務，屬機關業務類系統
	異動		



安全等級評估表範例(2/3)

「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：■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	
中	普	普	普	中
		資訊系統安全等級：		中

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	中	本系統資料屬敏感性資料，資料保護不當，將遭受一定程度之影響
	異動		
2. 完整性	初估	普	本系統目的在提供人事管理服務，不對外提供服務，若個人資料未妥適保存或發生資安事件造成資料外洩，可能造成資料完整性受損
	異動		
3. 可用性	初估	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業務運作
	異動		
4. 法律遵循性	初估	普	本系統包含同仁基本個人資料，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人資料保護法辦理資料保護，可能伴隨輕微不良後果
	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	行政類	本系統支援機關內部人事管理屬行政類資訊系統
	異動		



安全等級評估表範例(3/3)

「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：■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	
中	普	普	中	中
		資訊系統安全等級：		中

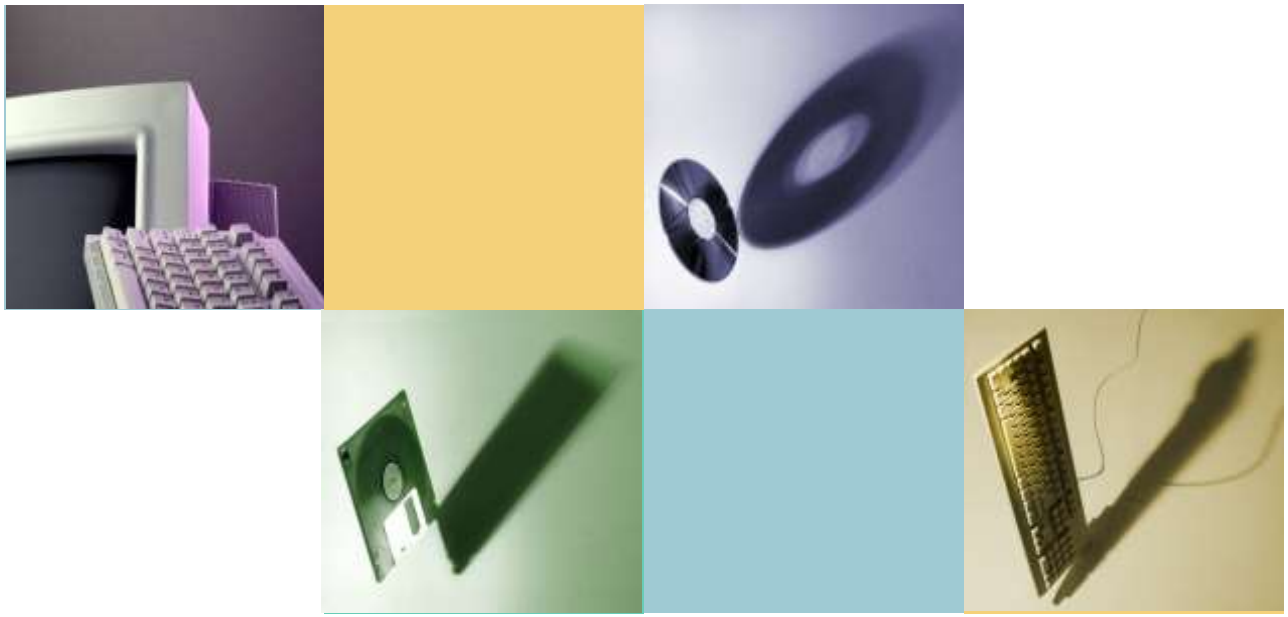
步驟❶：設定影響構面等級

影響構面		安全等級	原因說明
1. 機密性	初估	中	系統包含本機關收入、支出明細資料，屬敏感資料
	異動		
2. 完整性	初估	普	本系統目的在提供會計帳務管理，本系統不對外提供服務，惟會計帳務屬敏感性資料，若遭入侵完整性可能會有影響
	異動		
3. 可用性	初估	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業務運作
	異動		
4. 法律遵循性	初估	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		

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	行政類	本系統支援機關內部會計管理屬行政類資訊系統
	異動		





THANKS !