臺中市政府教育局

資訊安全教育訓練

(資通系統分級及防護基準)

漢昕科技
陳文奇 Benson

諮詢 輔導 訓練 稽核 . 永續營運

講師簡介— 陳文奇 Benson

- **證照**
  - Information Security Management Systems (ISMS) Auditor / Lead Auditor (in Accordance with ISO 27001:2013)
  - Information technology - Security techniques - Privacy framework Lead Auditor (in Accordance with ISO 29100:2011)
  - Personal Information Management Systems (PIMS, BS 10012:2017+A1:2018) Auditor/Lead Auditor
  - ITIL Foundation Certificate in IT Service Management
  - ECSA-FD Foundation Certification
- **經歷**
  - 漢昕科技股份有限公司 管理顧問處 顧問
  - 恩可埃技術服務有限公司 IT技術部/專案部 經理
  - 鑫品科技有限公司 業務工程師/專案經理
  - 典淳資訊股份有限公司 系統/網管 工程師
- **輔導實績**
  - 台灣自來水公司\臺灣港務公司\三軍總醫院\國家衛生研究院\車輛安全審驗中心\鯉魚潭給水廠...
  - 食品藥物管理署\核能研究所\關務署臺中關\水利規劃試驗所...
  - 雲林縣政府\台南市政府\嘉義市政府\臺中市政府地政局\臺中市政府教育局...
  - 國立台北藝術大學\國立臺灣體育運動大學\僑光科技大學\鉅冠印刷...

課程大綱

- 一、作業依據
- 二、流程說明
- 三、資通系統分級說明
- 四、防護基準說明

資通安全責任等級分級辦法–應辦事項

制度面向	辦理項目
管理面	資通系統分級及防護基準
	資訊安全管理系統之導入及通過公正第三方之驗證
	資通安全專責人員
	內部資通安全稽核
	業務持續運作演練

要做什麼呢?

- 初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統
  - —完成附表九資通系統分級
  - —完成附表十之控制措施
- 其後應每年至少檢視一次資通系統分級妥適性

免執行該事項或控制措施

- 條件
  - —技術限制
  - —個別資通系統之設計、結構或性質
  - —就特定事項或控制措施之辦理或執行顯有困難者
- 方式
  - —報請主管機關備查

第十一條　各機關應依其資通安全責任等級，辦理附表一至附表八之事項。

各機關自行或委外開發之資通系統應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表十所定資通系統防護基準執行控制措施；特定非公務機關之中央目的事業主管機關就特定類型資通系統之防護基準認有另為規定之必要者，得自行擬訂防護基準，報請主管機關核定後，依其規定辦理。

各機關辦理附表一至附表八所定事項或執行附表十所定控制措施，因技術限制、個別資通系統之設計、結構或性質等因素，就特定事項或控制措施之辦理或執行顯有困難者，得經第三條第二項至第四項所定其等級提交機關或同條第五項所定其等級核定機關同意，並報請主管機關備查後，免執行該事項或控制措施；其為主管機關者，經其同意後，免予執行。

公務機關之資通安全責任等級為 A 級或 B 級者，應依主管機關指定之方式，提報第一項及第二項事項之辦理情形。

中央目的事業主管機關得要求所管特定非公務機關，依其指定之方式提報第一項及第二項事項之辦理情形。

BCCS 漢昕科技 諮詢 輔導 訓練 稽核 .永續營運

課程大綱

一、作業依據

二、流程說明

三、資通系統分級說明

四、防護基準說明

流程說明

識別資通系統

資通系統清冊

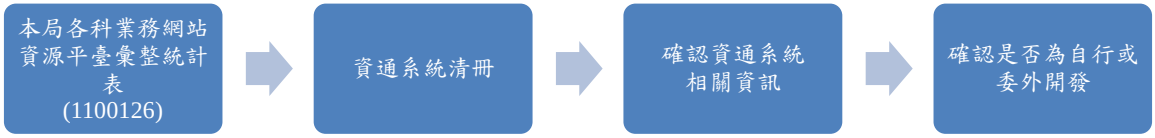
資通系統分級

資通系統安全等級評估表

套用防護基準

資通系統防護基準檢核表

識別資通系統



課程大綱

BCCS 漢昕科技
諮詢 輔導 訓練 稽核 . 永續營運

使用表單

「_____系統」安全等級評估表

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

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：識別資通屬性

項目		資通屬性	原因說明
識別資通屬性	初估		
	異動		
備註			

資通系統開發		資訊系統開發	
系統人	業管主管	系統人	業管主管

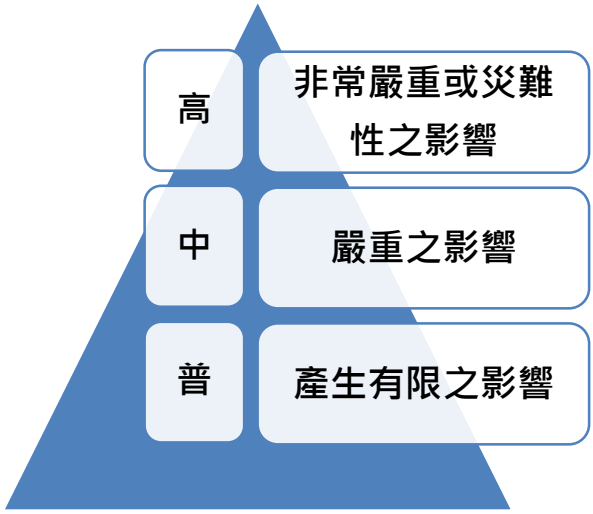
1. 設定影響構面等級

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

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		

安全等級



影響構面等級–機密性

防護需求等級 / 構面	高	中	普
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響

BCCS 漢昕科技
諮詢 輔導 訓練 稽核 .永續營運

影響構面等級–完整性

防護需求等級 構面	高	中	普
完整性	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事對機關之營運、資產或信譽等方面將產生有限之影響。

影響構面等級–可用性

防護需求等級 構面	高	中	普
可用性	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。

影響構面等級–法律遵循性

防護需求等級 構面	高	中	普
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規範之情形

2. 識別業務屬性

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			

3. 簽核

業務承辦單位		資訊承辦單位	
承辦人	直屬主管	承辦人	直屬主管

課程大綱

- 一、作業依據
- 二、流程說明
- 三、資通系統分級說明
- 四、防護基準說明

BCCS 漢昕科技 諮詢 輔導 訓練 稽核 . 永續營運

防護基準

7個構面、29項控制措施類別

構面	控制措施類別
存取控制	帳號管理/最小權限/遠端存取
稽核與可歸責性	稽核事件/稽核紀錄內容/稽核儲存容量/稽核處理失效之回應/時戳及校時/稽核資訊之保護
營運持續計畫	系統備份/系統備援
識別與鑑別	內部使用者之識別與鑑別/身分驗證管理/鑑別資訊回饋/加密模組鑑別/非內部使用者之識別與鑑別
系統與服務獲得	系統發展生命週期需求階段/開發階段/測試階段/部署與維運階段/委外階段/獲得程序/系統文件
系統與通訊保護	傳輸之機密性與完整性/資料儲存之安全
系統與資訊完整性	漏洞修復/資通系統監控/軟體及資訊完整性

檢核說明

2.系統防護評量

普、中、高級系統適用項目

中、高級以上系統適用項目

高級系統適用項目

BCCS 漢昕科技 諮詢 輔導 訓練 稽核 . 永續營運

存取控制

存取控制-帳號管理

安全等級		
高	中	普
逾越機關所定預期閒置時間或可使用期限時，系統應自動將使用者登出	已逾期之臨時或緊急帳號應刪除或禁用	建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序
應依機關規定之情況及條件，使用資通系	資通系統閒置帳號應禁用	
監控資通系統帳號，如發現帳號違常使用時回報管理者	定期審核資通系統帳號之建立、修改、啟用、禁用及刪除。	
等級「中」之所有控制措施	等級「普」之所有控制措施。	

BCCS 漢昕科技
諮詢 輔導 訓練 稽核 .永續營運

存取控制-最小權限

安全等級		
高	中	普
採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。		無要求

存取控制-遠端存取

安全等級		
高	中	普
應監控資通系統遠端連線		對於每一種允許之 遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化，使用者之權限檢查作業應於伺服器端完成
資通系統應採用加密機制		
資通系統遠端存取之來源應為機關已預先定義及管理之存取控制點		
等級「普」之所有控制措施		

稽核與可歸責性

稽核與可歸責性-稽核事件

安全等級		
高	中	普
應定期審查稽核事件		依規定時間週期及紀錄留存政策，保留稽核紀錄
等級「普」之所有控制措施		確保資通系統有稽核特定事件之功能，並決定應稽核之特定資通系統事件
		應稽核資通系統管理者帳號所執行之各項功能

BCCS 漢昕科技
諮詢 輔導 訓練 稽核 .永續營運

稽核與可歸責性-稽核紀錄內容

安全等級		
高	中	普
資通系統產生之稽核紀錄，應依需求納入其他相關資訊		資通系統產生之稽核紀錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用單一日誌紀錄機制，確保輸出格式之一致性
等級「普」之所有控制措施		

稽核與可歸責性-稽核儲存容量

安全等級		
高	中	普
依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量		

稽核與可歸責性-稽核處理失效之回應

安全等級		
高	中	普
機關規定需要即時通報之稽核失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。	資通系統於稽核處理失效時，應採取適當之行動	
等級「中」及「普」之所有控制措施。		

稽核與可歸責性-時戳及校時

安全等級		
高	中	普
系統內部時鐘應依機關規定之時間週期與基準時間源進行同步		資通系統應使用系統內部時鐘產生稽核紀錄所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。
等級「普」之所有控制措施		

稽核與可歸責性-稽核資訊之保護

安全等級		
高	中	普
定期備份稽核紀錄至與原稽核系統不同之實體系統。	應運用雜湊或其他適當方式之完整性確保機制。	對稽核紀錄之存取管理，僅限於有權限之使用者。
等級「中」之所有控制措施。	等級「普」之所有控制措施	

營運持續計畫

營運持續計畫-系統備份

安全等級		
高	中	普
應將備份還原，作為營運持續計畫測試之一部分	應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性	訂定系統可容忍資料損失之時間要求
應在與運作系統不同處之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份	等級「普」之所有控制措施	執行系統源碼與資料備份
等級「中」之所有控制措施		

營運持續計畫-系統備援

安全等級		
高	中	普
訂定資通系統從中斷後至重新恢復服務之可容忍時間要求		無要求。
原服務中斷時，於可容忍時間內，由備援設備取代提供服務		

識別與鑑別

識別與鑑別-內部使用者之識別與鑑別

安全等級		
高	中	普
對帳號之網路或本機存取採取多重認證技術	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號	
等級「中」及「普」之所有控制措施。		

BCCS 漢昕科技
諮詢 輔導 訓練 稽核 .永續營運

識別與鑑別-身分驗證管理

安全等級		
高	中	普
身分驗證機制應防範自動化程式之登入或密碼更換嘗試		使用預設密碼登入系統時，應於登入後要求立即變更
密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記		身分驗證相關資訊不以明文傳輸
等級「普」之所有控制措施		具備帳戶鎖定機制，帳號登入進行身分驗證失敗達三次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制
		基於密碼之鑑別資通系統應強制最低密碼複雜度；強制密碼最短及最長之效期限制。
		使用者更換密碼時，至少不可以與前三次使用過之密碼相同
		第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理

識別與鑑別-鑑別資訊回饋

安全等級		
高	中	普
資通系統應遮蔽鑑別過程中之資訊		

識別與鑑別-鑑別資訊回饋

安全等級		
高	中	普
資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存		無要求。

識別與鑑別-非內部使用者之識別與鑑別

安全等級		
高	中	普
資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。		

系統與服務獲得

系統與服務獲得-系統發展生命週期需求階段

安全等級		
高	中	普
針對系統安全需求（含機密性、可用性、完整性），以檢核表方式進行確認		

BCCS 漢昕科技
諮詢 輔導 訓練 稽核 .永續營運

系統與服務獲得-系統發展生命週期設計階段

安全等級		
高	中	普
根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估		無要求
將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正		

系統與服務獲得-系統發展生命週期開發階段

安全等級		
高	中	普
執行「源碼掃描」安全檢測	應針對安全需求實作必要控制措施	
具備系統嚴重錯誤之通知機制。	應注意避免軟體常見漏洞及實作必要控制措施	
等級「中」及「普」之所有控制措施	發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息	

系統與服務獲得-系統發展生命週期測試階段

安全等級		
高	中	普
執行「滲透測試」安全檢測	執行「弱點掃描」安全檢測。	
等級「中」及「普」之所有控制措施		

系統與服務獲得-系統發展生命週期部署與維運階段

安全等級		
高	中	普
於系統發展生命週期之維運階段，須注意版本控制與變更管理		於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口
等級「普」之所有控制措施		資通系統相關軟體，不使用預設密碼。

系統與服務獲得-系統發展生命週期委外階段

安全等級		
高	中	普
資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約		

系統與服務獲得-獲得程序

安全等級		
高	中	普
開發、測試及正式作業環境應為區隔		無要求

系統與服務獲得-系統文件

安全等級		
高	中	普
應儲存與管理系統發展生命週期之相關文件。		

系統與通訊保護

系統與通訊保護-傳輸之機密性與完整性

安全等級		
高	中	普
資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。	無要求	
使用公開、國際機構驗證且未遭破解之演算法。		
支援演算法最大長度金鑰。		
加密金鑰或憑證週期性更換。		
伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施		

系統與通訊保護-資料儲存之安全

安全等級		
高	中	普
靜置資訊及相關具保護需求之機密資訊應加密儲存。	無要求	

靜置資訊：指資訊位於資通系統特定元件，例如儲存設備上之狀態，或與系統相關需要保護之資訊，例如設定防火牆、閘道器、入侵偵測、防禦系統、過濾式路由器及鑑別符內容等資訊。

系統與資訊完整性

系統與資訊完整性-漏洞修復

安全等級		
高	中	普
定期確認資通系統相關漏洞修復之狀態		系統之漏洞修復應測試有效性及潛在影響，並定期更新
等級「普」之所有控制措施		

BCCS 漢昕科技
諮詢 輔導 訓練 稽核 . 永續營運

系統與資訊完整性-資通系統監控

安全等級		
高	中	普
資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析	監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用	發現資通系統有被入侵跡象時，應通報機關特定人員
等級「中」之所有控制措施	等級「普」之所有控制措施	

系統與資訊完整性-軟體及資訊完整性

安全等級		
高	中	普
應定期執行軟體與資訊完整性檢查	使用完整性驗證工具，以偵測未授權變更特定軟體及資訊	無要求
等級「中」之所有控制措施	使用者輸入資料合法性檢查應置放於應用系統伺服器端	
	發現違反完整性時，資通系統應實施機關指定之安全保護措施	

Thank You

感謝聆聽 敬請指教

陳文奇 Benson

benson@bccs.com.tw