僑光科技大學
110學年度資訊系統防護基準線上說明會

線上說明會

陳泰龍 Felix

- **證照**
  - Information Security Management Systems (ISMS) Auditor / Lead Auditor (in Accordance with ISO 27001:2013)
- **經歷**
  - 漢昕科技股份有限公司　管理顧問處 顧問
  - 德誼科技股份有限公司　蘋果電腦維修工程師
  - 台灣大哥大股份有限公司 業務代表
- **輔導實績**

  新竹縣政府\台中市教育局資訊教育暨網路中心 \僑光科技大學\嘉義縣環境保護局\大葉大學、中部汽車股份有限公司、金統立工業股份有限公司教育訓練\台灣自來水公司內部稽核\臺東專科學校、大葉大學內部稽核

課程大綱

一、源起

二、安全等級評估表

三、資訊系統清冊

四、資安防護基準檢核表

課程大綱

一、源起

二、安全等級評估表

三、資訊系統清冊

四、資安防護基準檢核表

一、源起

教育體系資通安全暨個人資料管理規範

應參考「資通安全責任等級分級辦法」附表九資通系統防護需求分級原則，鑑別適用範圍內資訊系統之安全等級，資訊系統經鑑別後，其安全等級屬最高等級者，應執行風險評估、擬訂與執行風險管理措施；其安全等級非屬最高等級者，應衡酌其風險程度，以決定是否進行風險評估、擬訂與執行風險管理措施

一、源起

資通安全管理法-附表三資通安全責任等級B級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		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，依附表九完成資通系統分級，並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。
	資訊安全管理系統之導入及通過公正第三方之驗證		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置二人；須以專職人員配置之。
	內部資通安全稽核		每年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。
	資安治理成熟度評估		每年辦理一次。

課程大綱

一、源起

二、安全等級評估表

三、資訊系統清冊

四、資安防護基準檢核表

各資訊系統均須依循處理程序填寫「安全等級評估表」

步驟1

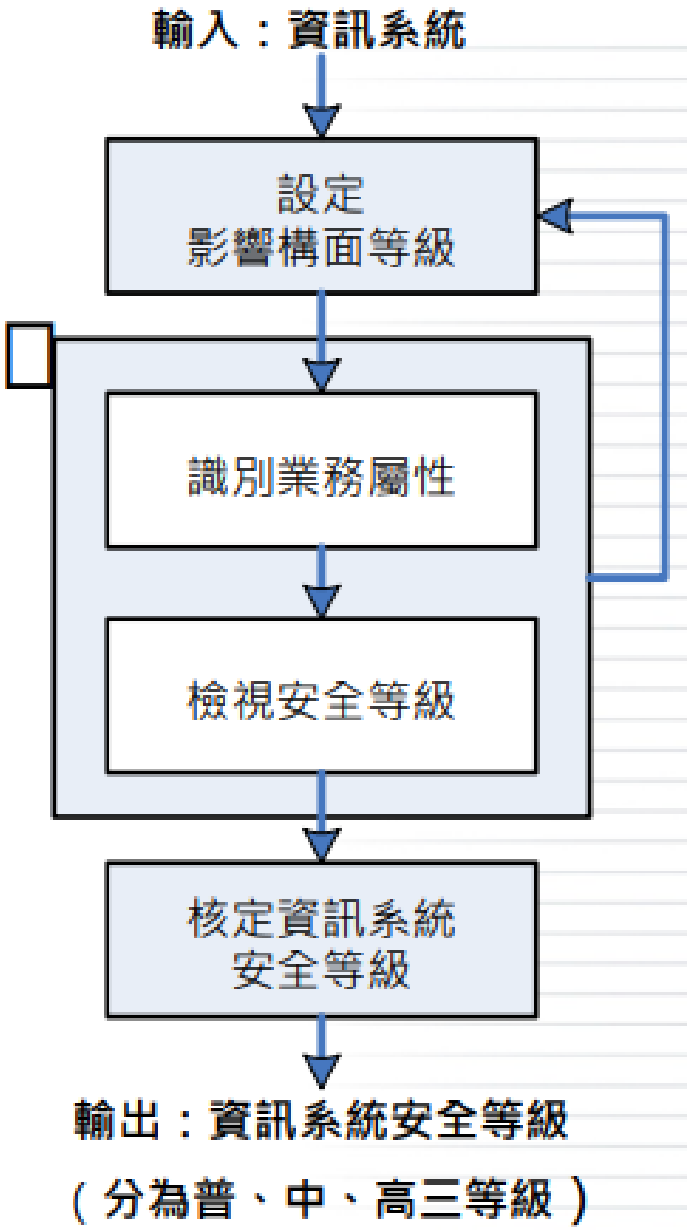
依機密性、完整性、可用性及法律遵循性四大 構面，分別評估對各資訊系統（不含共同性系統）之影響衝擊，並設定影響構面等級，依資訊系統填寫「安全等級 評估表」

步驟2

依據資訊系統支援之業務屬性（分為行政與業務二類），檢視安全等級之合理性

步驟3

由資訊單位將各資訊系統「安全等級評估表」中資訊，併同共同性系統，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，由資通安全長核定。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。



構面 \ 等級	普	中	高
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，對本〇之營運、資產或信譽等方面將產生有限之影響， 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。	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，對本〇之營運、資產或信譽等方面將產生嚴重之影響， 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。	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，對本〇之營運、資產或信譽等方面將產生非常嚴重或災難性之影響， 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。極大規模（如：全國性）之涉及識別個人之資料。例如： 戶役政資訊系統、護照管理 系統等

構面 \ 等級	普	中	高
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，對本校之營運、資產或信譽等方面將產生有限之影響。	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，對本校之營運、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，對本校之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。
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，對本校之營運、資產或信譽等方面將產生有限之影響，如： 系統容許中斷時間較長（如：48、72小時）。系統故障造成機關業務 執行效能輕微降低。	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，對本校之營運、資產或信譽等方面將產生嚴重之影響，如： 系統容許中斷時間短（如：12、24小時）。系統故障造成機關業務執行效能嚴重降低。	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，對本校之營運、資產或信譽等方面將產生非常嚴重或災難性之影響，如： 系統容許中斷時間非常短（如：4、8小時）。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

構面 \ 等級	普	中	高
法律遵循性	其他資通系統設置或運作於法令有相關規範之情形如： 全球資訊網：必須符合智慧財產權相關法令尊重他人智慧結晶，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	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本校執行業務之公正性及正當性，並使本校或其所屬人員受行政罰、懲戒或懲處，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。	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本校執行業務之公正性及正當性，並使本校所屬人員負刑事責任，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。

二、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	● 共同性系統類別：☐共用性(單位僅涉及使用操作) ☐共通性(資料主要儲存於單位) ☐非共同性系統 ● 系統建置方式：☐自行委外 ☐租用服務 ☐套裝軟體 ☐自行開發 ☐主管/上級機關提供 ☐其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：請各機關依本身實際陳核流程調整簽核欄位

建議對照「資訊系統清冊」編號欄位

編號	資訊系統名稱	業務屬性	安全等級	系統建置方式	共同性系統(Y/N)	承辦(管理)單位	備註
01							
02							
03							
04							

二、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	● 共同性系統類別:□共用性(單位僅涉及使用操作) □共通性(資料主要儲存於單位) □非共同性系統 ● 系統建置方式:□自行委外 □租用服務 □套裝軟體 □自行開發 □主管/上級機關提供 □其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：請各機關依本身實際陳核流程調整簽核欄位

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。

二、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	● 共同性系統類別:□共用性(單位僅涉及使用操作) □共通性(資料主要儲存於單位) □非共同性系統 ● 系統建置方式:□自行委外 □租用服務 □套裝軟體 □自行開發 □主管/上級機關提供 □其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：請各機關依本身實際陳核流程調整簽核欄位

建議功能說明內容參考範例

一、停車管理系統

提供停車場所查詢，以及汽機車未繳費資料查詢線上服務。

二、全球資訊網

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。

三、人事管理系統

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。

四、會計管理系統

提供機關會計人員進行會計帳務作業及管理。

二、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	● 共同性系統類別:☐共用性(單位僅涉及使用操作) ☐共通性(資料主要儲存於單位) ☐非共同性系統 ● 系統建置方式:☐自行委外 ☐租用服務 ☐套裝軟體 ☐自行開發 ☐主管/上級機關提供 ☐其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：請各機關依本身實際陳核流程調整簽核欄位

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）。

二、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	● 共同性系統類別：□共用性(單位僅涉及使用操作) □共通性(資料主要儲存於單位) □非共同性系統 ● 系統建置方式：□自行委外 □租用服務 □套裝軟體 □自行開發 □主管/上級機關提供 □其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：請各機關依本身實際陳核流程調整簽核欄位

二、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	● 共同性系統類別:☐共用性(單位僅涉及使用操作) ☐共通性(資料主要儲存於單位) ☐非共同性系統 ● 系統建置方式:☐自行委外 ☐租用服務 ☐套裝軟體 ☐自行開發 ☐主管/上級機關提供 ☐其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：請各機關依本身實際陳核流程調整簽核欄位

建議承辦單位主管對於承辦人員所填之「初估」資料有變更，可將內容填至「異動」欄位進行註記。

二、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	● 共同性系統類別:☐共用性(單位僅涉及使用操作) ☐共通性(資料主要儲存於單位) ☐非共同性系統 ● 系統建置方式:☐自行委外 ☐租用服務 ☐套裝軟體 ☐自行開發 ☐主管/上級機關提供 ☐其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：請各機關依本身實際陳核流程調整簽核欄位

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。

二、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	● 共同性系統類別:□共用性(單位僅涉及使用操作) □共通性(資料主要儲存於單位) □非共同性系統 ● 系統建置方式:□自行委外 □租用服務 □套裝軟體 □自行開發 □主管/上級機關提供 □其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：請各機關依本身實際陳核流程調整簽核欄位

建議採用以下辨識方法，避免機關內出現過多判定系統安全等級【高】之系統，導致資源誤用之情形。

構面 \ 安全等級	是否會上媒體【頭版頭條】	媒體【內頁資訊】	【不會上媒體】
資料被竊	高	中	普
資料被修改	高	中	普
資訊系統當機或停止服務	高	中	普
具有法律爭議問題時	高	中	普

二、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	● 共同性系統類別:□共用性(單位僅涉及使用操作) □共通性(資料主要儲存於單位) □非共同性系統 ● 系統建置方式:□自行委外 □租用服務 □套裝軟體 □自行開發 □主管/上級機關提供 □其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：請各機關依本身實際陳核流程調整簽核欄位

建議原因說明內容參考範例

一、停車管理系統

(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。

二、全球資訊網

(普)網站資訊均為可公開之一般性資料。

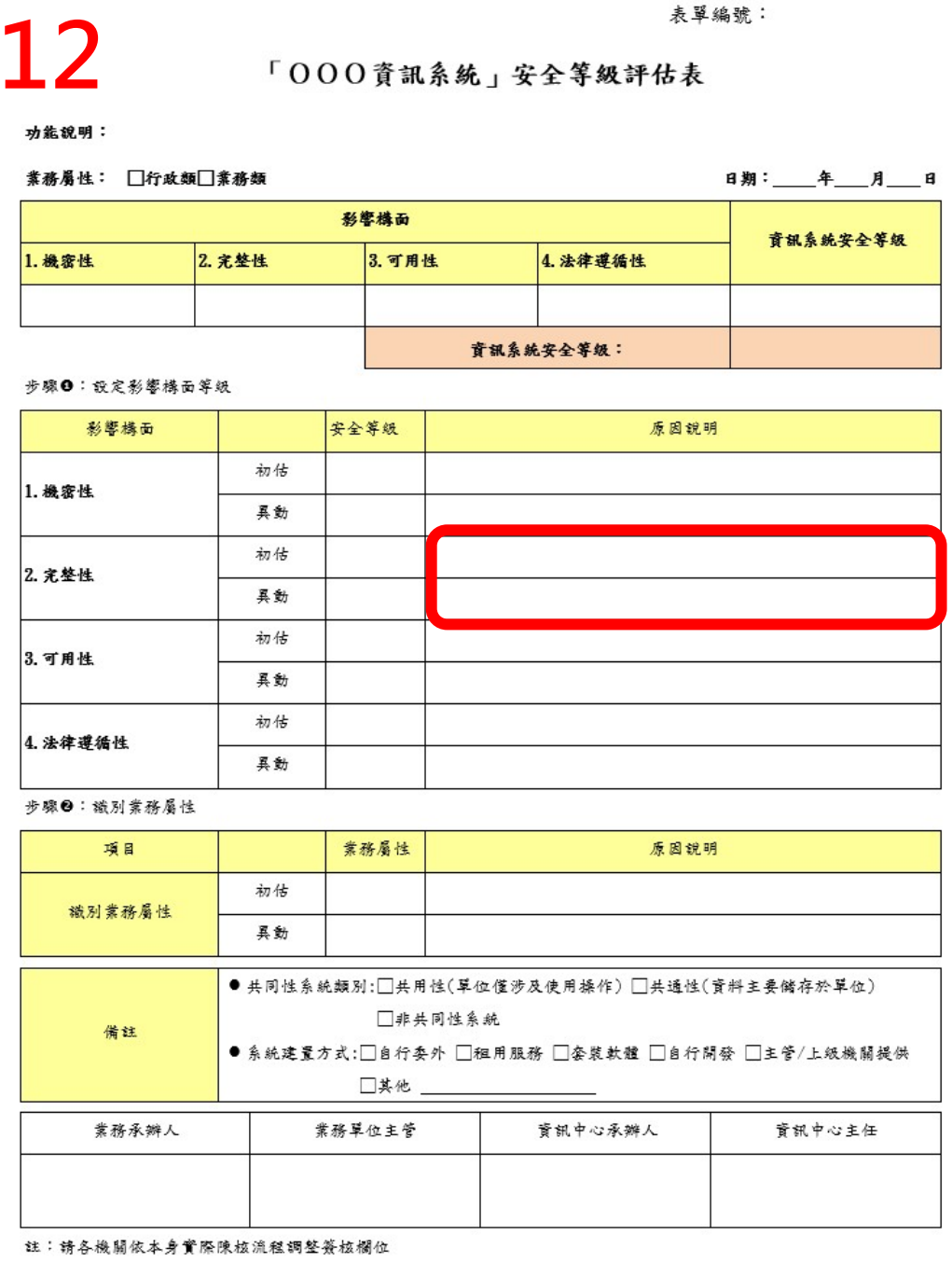
三、人事管理系統

(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。

四、會計管理系統

(中)系統包含本機關收入、支出明細資料，屬敏感資料。

二、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	● 共同性系統類別:□共用性(單位僅涉及使用操作) □共通性(資料主要儲存於單位) □非共同性系統 ● 系統建置方式:□自行委外 □租用服務 □套裝軟體 □自行開發 □主管/上級機關提供 □其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：請各機關依本身實際陳核流程調整簽核欄位

建議原因說明內容參考範例

一、停車管理系統

(高)本系統目的在提供車輛未繳費資料查詢服務，若資料未妥適保存或發生資安事件造成資料缺漏，可能造成資料完整性受損。

二、全球資訊網

(普)本網站主要提供資訊公告。

三、人事管理系統

(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遭竄改，可能造成資料完整性受損。

四、會計管理系統

(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，若遭駭客入侵並移除帳務資料，完整性可能會有影響。

二、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	● 共同性系統類別:☐共用性(單位僅涉及使用操作) ☐共通性(資料主要儲存於單位) ☐非共同性系統 ● 系統建置方式:☐自行委外 ☐租用服務 ☐套裝軟體 ☐自行開發 ☐主管/上級機關提供 ☐其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：請各機關依本身實際陳核流程調整簽核欄位

建議原因說明內容參考範例

一、停車管理系統

(普)本系統容許中斷時間較長(72小時)，且服務中斷不致影響業務運作。

二、全球資訊網

(普)本網站提供一般性資料瀏覽，容許中斷時間較長(48小時)，且服務中斷不致影響業務運作。

三、人事管理系統

(普)本系統容許中斷時間較長(24小時)，且服務中斷不致影響業務運作。

四、會計管理系統

(普)本系統容許中斷時間較長(24小時)，且服務中斷不致影響業務運作。

二、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	● 共同性系統類別:□共用性(單位僅涉及使用操作) □共通性(資料主要儲存於單位) □非共同性系統 ● 系統建置方式:□自行委外 □租用服務 □套裝軟體 □自行開發 □主管/上級機關提供 □其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：請各機關依本身實際陳核流程調整簽核欄位

建議原因說明內容參考範例

一、停車管理系統

(中)本系統資料包含車號與未繳費資料明細等，應依「個人資料保護法」規定辦理。

二、全球資訊網

(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。

三、人事管理系統

(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。

四、會計管理系統

(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。

二、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	● 共同性系統類別:□共用性(單位僅涉及使用操作) □共通性(資料主要儲存於單位) □非共同性系統 ● 系統建置方式:□自行委外 □租用服務 □套裝軟體 □自行開發 □主管/上級機關提供 □其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：請各機關依本身實際陳核流程調整簽核欄位

若兩欄位皆有內容，則資訊系統安全等級以「異動」欄位為主。

二、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		

備註	● 共同性系統類別：□共用性(單位僅涉及使用操作) □共通性(資料主要儲存於單位) □非共同性系統 ● 系統建置方式：□自行委外 □租用服務 □套裝軟體 □自行開發 □主管/上級機關提供 □其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：請各機關依本身實際陳核流程調整簽核欄位

取其四大影響構面安全等級**最高者**。

17

二、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	● 共同性系統類別:□共用性(單位僅涉及使用操作) □共通性(資料主要儲存於單位) □非共同性系統 ● 系統建置方式:□自行委外 □租用服務 □套裝軟體 □自行開發 □主管/上級機關提供 □其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：請各機關依本身實際陳核流程調整簽核欄位

二、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

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	● 共同性系統類別:□共用性(單位僅涉及使用操作) □共通性(資料主要儲存於單位) □非共同性系統 ● 系統建置方式:□自行委外 □租用服務 □套裝軟體 □自行開發 □主管/上級機關提供 □其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：請各機關依本身實際陳核流程調整簽核欄位

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）。

二、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	● 共同性系統類別:□共用性(單位僅涉及使用操作) □共通性(資料主要儲存於單位) □非共同性系統 ● 系統建置方式:□自行委外 □租用服務 □套裝軟體 □自行開發 □主管/上級機關提供 □其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：請各機關依本身實際陳核流程調整簽核欄位

建議原因說明內容參考範例

一、停車管理系統

(業務類)本系統提供汽機車未繳費資料查詢等對外資訊服務，屬機關業務類系統。

二、全球資訊網

(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。

三、人事管理系統

(行政類)本系統支援機關內部人事管理屬行政類資訊系統。

四、會計管理系統

(行政類)本系統支援機關內部會計管理屬行政類資訊系統。

二、安全等級評估表

共同性系統類別

■共用性(單位僅涉及使用操作)

□共通性(資料主要儲存於單位) ■非共同性系統

系統建置方式

□自行委外 □租用服務 □套裝軟體 ■自行開發

■主管/上級機關提供 □其他

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	● 共同性系統類別：□共用性(單位僅涉及使用操作) □共通性(資料主要儲存於單位) □非共同性系統 ● 系統建置方式：□自行委外 □租用服務 □套裝軟體 □自行開發 □主管/上級機關提供 □其他 _____		

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

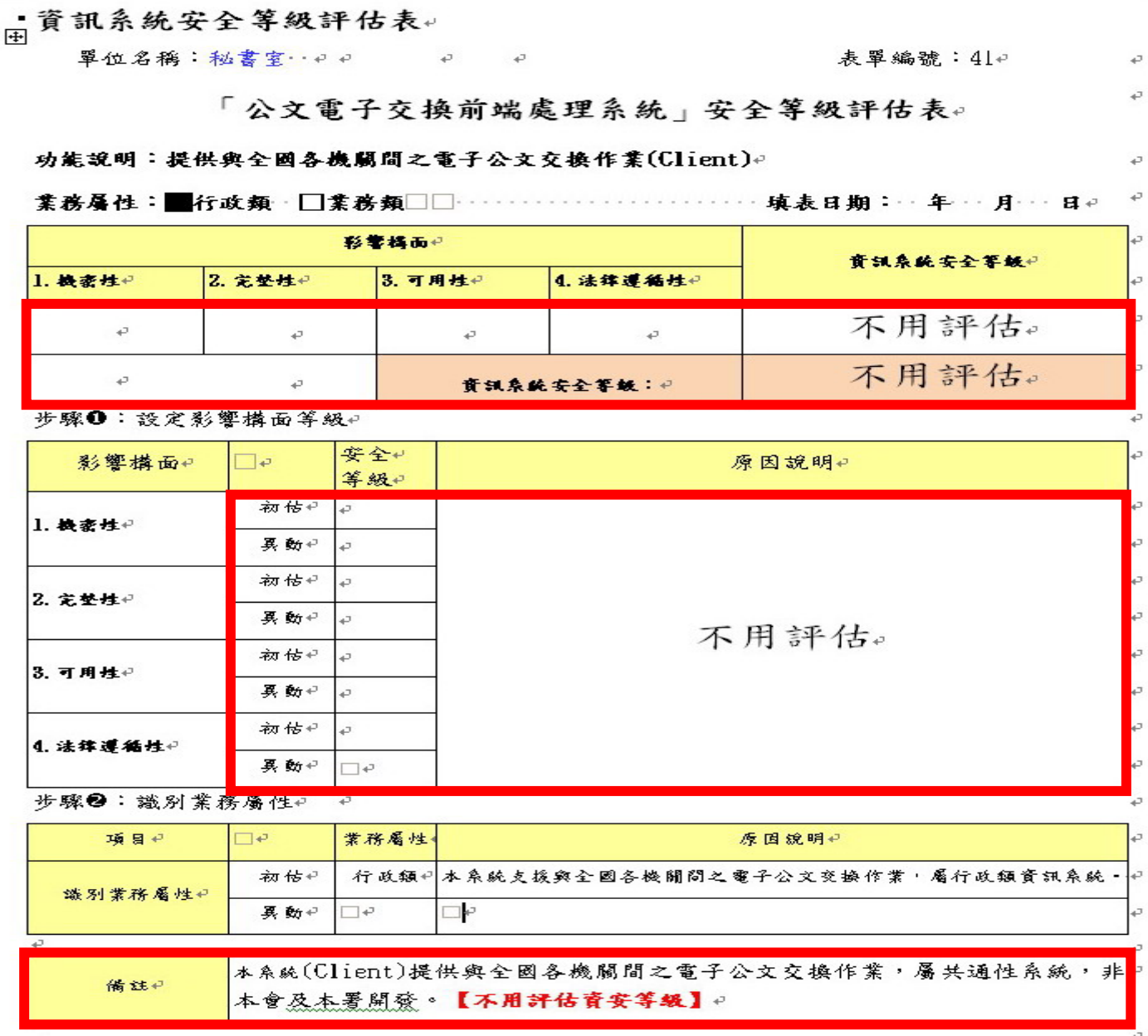
註：請各機關依本身實際陳核流程調整簽核欄位

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訂，其餘機關除使用操作外，資料主要儲存於使用機關。

二、安全等級評估表



▪資訊系統安全等級評估表

單位名稱：秘書室　　表單編號：41

「公文電子交換前端處理系統」安全等級評估表

功能說明：提供與全國各機關間之電子公文交換作業(Client)

業務屬性：■行政類 □業務類□□　　填表日期：　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	
				不用評估
		資訊系統安全等級：		不用評估

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		不用評估
	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	行政類	本系統支援與全國各機關間之電子公文交換作業，屬行政類資訊系統。
	異動	□	□

備註	本系統(Client)提供與全國各機關間之電子公文交換作業，屬共通性系統，非本會及本署開發。【不用評估資安等級】

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

二、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	● 共同性系統類別：□共用性(單位僅涉及使用操作) □共通性(資料主要儲存於單位) □非共同性系統 ● 系統建置方式：□自行委外 □租用服務 □套裝軟體 □自行開發 □主管/上級機關提供 □其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：請各機關依本身實際陳核流程調整簽核欄位

本處理程序須由業務承辦人、業務單位主管、資訊中心承辦人、資訊中心主任等相關人員會辦，最後彙整至資訊系統清冊由資訊安全長核定資訊系統安全等級。

建議「安全等級評估表」簽核欄位如下：

一、業務承辦人

二、業務單位主管

三、資訊中心承辦人員

四、資訊中心主任

課程大綱

一、源起

二、安全等級評估表

三、資訊系統清冊

四、資安防護基準檢核表

01

三、資訊系統清冊

表單編號：01

僑光科技大學資訊系統清冊

彙整日期：　年　月　日

編號	資訊系統名稱	業務屬性	安全等級	系統建置方式	共同性系統(Y/N)	承辦(管理)單位	備註
12							
13							
14							
15							
16							
17							

承辦單位承辦人	承辦單位主管	決行(資安長)

02

三、資訊系統清冊

表單編號：01

僑光科技大學資訊系統清冊

彙整日期：　年　月　日

編號	資訊系統名稱	業務屬性	安全等級	系統建置方式	共同性系統(Y/N)	承辦(管理)單位	備註
12							
13							
14							
15							
16							
17							
承辦單位承辦人		承辦單位主管			決行(資安長)		

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	
備註	● 共同性系統類別：□共用性(單位僅涉及使用操作) □共通性(資料主要儲存於單位) □非共同性系統 ● 系統建置方式：□自行委外 □租用服務 □套裝軟體 □自行開發 □主管/上級機關提供 □其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：各機關依本身實際陳核流程調整簽核欄位

03

三、資訊系統清冊

表單編號：01

僑光科技大學資訊系統清冊

彙整日期：　年　月　日

編號	資訊系統名稱	業務屬性	安全等級	系統建置方式	共同性系統 (Y/N)	承辦(管理)單位	備註
12							
13							
14							
15							
16							
17							
承辦單位承辦人		承辦單位主管			決行(資安長)		

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	
	● 共同性系統類別：□共用性(單位僅涉及使用操作) □共通性(資料主要儲存於單位) □非共同性系統 ● 系統建置方式：□自行委外 □租用服務 □套裝軟體 □自行開發 □主管/上級機關提供 □其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：請各機關依本身實際陳核流程調整簽核欄位

04

三、資訊系統清冊

表單編號：01

僑光科技大學資訊系統清冊

簽署日期：　年　月　日

編號	資訊系統名稱	業務屬性	安全等級	系統建置方式	共同性系統(Y/N)	承辦(管理)單位	備註
12							
13							
14							
15							
16							
17							
承辦單位承辦人		承辦單位主管			決行(資安長)		

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	
備註	● 共同性系統類別:☐共用性(單位僅涉及使用操作) ☐共通性(資料主要儲存於單位) ☐非共同性系統 ● 系統建置方式:☐自行委外 ☐租用服務 ☐套裝軟體 ☐自行開發 ☐主管/上級機關提供 ☐其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

：請各機關依本身實際陳核流程調整簽核欄位

05

三、資訊系統清冊

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	● 共同性系統類別:☐共用性(單位僅涉及使用操作) ☐共通性(資料主要儲存於單位) ☐非共同性系統 ● 系統建置方式:☐自行委外 ☐租用服務 ☐套裝軟體 ☐自行開發 ☐主管/上級機關提供 ☐其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：請各機關依本身實際陳核流程調整簽核欄位

表單編號：01

僑光科技大學資訊系統清冊

彙整日期：　年　月　日

編號	資訊系統名稱	業務屬性	安全等級	系統建置方式	共同性系統(Y/N)	承辦(管理)單位	備註
12							
13							
14							
15							
16							
17							
承辦單位承辦人		承辦單位主管			決行(資安長)		

05

三、資訊系統清冊

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	● 共同性系統類別：□共用性(單位僅涉及使用操作) □共通性(資料主要儲存於單位) □非共同性系統 ● 系統建置方式：□自行委外 □租用服務 □套裝軟體 □自行開發 □主管/上級機關提供 □其他 _____

業務承辦人	業務單位主管	資訊中心承辦人	資訊中心主任

註：請各機關依本身實際陳核流程調整簽核欄位

表單編號：01

僑光科技大學資訊系統清冊

彙整日期：　年　月　日

編號	資訊系統名稱	業務屬性	安全等級	系統建置方式	共同性系統(Y/N)	承辦(管理)單位	備註
12							
13							
14							
15							
16							
17							
承辦單位承辦人		承辦單位主管			決行(資安長)		

三、資訊系統清冊

表單編號：01

僑光科技大學資訊系統清冊

彙整日期：　年　月　日

編號	資訊系統名稱	業務屬性	安全等級	系統建置方式	共同性系統(Y/N)	承辦(管理)單位	備註
12							
13							
14							
15							
16							
17							

承辦單位承辦人	承辦單位主管	決行(資安長)

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訂，其餘機關除使用操作外，資料主要儲存於使用機關。

三、資訊系統清冊

表單編號：01

僑光科技大學資訊系統清冊

彙整日期：　年　月　日

編號	資訊系統名稱	業務屬性	安全等級	系統建置方式	共同性系統(Y/N)	承辦(管理)單位	備註
12							
13							
14							
15							
16							
17							

承辦單位承辦人	承辦單位主管	決行(資安長)

建議「資訊系統清冊」簽核欄位如下：

一、資訊安全承辦人員

二、資訊安全承辦單位主管

三、資訊安全長

課程大綱

一、源起

二、安全等級評估表

三、資訊系統清冊

四、資安防護基準檢核表

四、資安防護基準檢核表

資訊系統分級與資安防護基準作業規定

機關完成資訊系統分級後，應依資訊系統【高】、【中】、【普】等級，執行相對應之防護基準。即【高】等級資訊系統執行高等級防護措施，【中】、【普】等級資訊系統，則執行【中】、【普】等級防護措施。機關可依其資源，調整控制措施之優先順序。

四、資安防護基準檢核表

資訊系統分級與資安防護基準作業規定

附表十　資通系統防護基準

系統防護需求分級 控制措施		高	中	普
構面	措施內容			
存取控制	帳號管理	一、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。 二、應依機關規定之情況及條件，使用資通系統。 三、監控資通系統帳號，如發現帳號違常使用時回報管理者。 四、等級「中」之所有控制措施。	一、已逾期之臨時或緊急帳號應刪除或禁用。 二、資通系統閒置帳號應禁用。 三、定期審核資通系統帳號之建立、修改、啟用、禁用及刪除。 四、等級「普」之所有控制措施。	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。
	最小權限	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。

四、資安防護基準檢核表

資訊系統防護基準控制措施查檢表

資通系統防護基準法令依據

【資通安全責任等級分級辦法 第十一條】

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...。

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**... 。

資通系統防護基準法令依據

【資通安全責任等級分級辦法 第十一條】

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**...。

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 。

資通系統防護基準控制措施說明

【存取控制-帳號管理】【中】

1.已逾期之臨時或緊急帳號應刪除或禁用。

資通系統防護基準控制措施說明

【存取控制-帳號管理】【中】

2.資通系統閒置帳號應禁用。

資通系統防護基準控制措施說明

【存取控制-帳號管理】【中】

3.定期審核資通系統帳號之建立、修改、啟用、禁用及刪除。

資通系統防護基準控制措施說明

【存取控制-帳號管理】【中】【普】

4.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。

資通系統防護基準控制措施說明

【存取控制-最小權限】【中】

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。

資通系統防護基準控制措施說明

【存取控制-遠端存取】【中】

1.應監控資通系統遠端連線。

資通系統防護基準控制措施說明

【存取控制-遠端存取】【中】

2.資通系統應採用加密機制。

□VPN □SFTP □https

資通系統防護基準控制措施說明

【存取控制-遠端存取】【中】

3.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。

資通系統防護基準控制措施說明

【存取控制-遠端存取】【中】【普】

4.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。

資通系統防護基準控制措施說明

【存取控制-遠端存取】【普】

4.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。

行政院技服中心建議 107.11.15

1. 未登入系統帳號情況下，試圖存取非公開頁面會被系統拒絕。
2. 停用瀏覽器JavaScript功能後，以一般使用者帳號登入，試圖存取管理者頁面功能，系統應拒絕存取。

資通系統防護基準控制措施說明

【稽核與可歸責性-稽核事件】

1.應定期審查稽核事件。【中】

【稽核與可歸責性-稽核紀錄內容】

2.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。

資通系統防護基準控制措施說明

【稽核與可歸責性-稽核事件】

2.依規定時間週期及紀錄留存政策，保留稽核紀錄。

【中】【普】

資通系統防護基準控制措施說明

【稽核與可歸責性-稽核事件】

3.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。【中】【普】

【稽核與可歸責性-稽核紀錄內容】

2.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。

資通系統防護基準控制措施說明

【稽核與可歸責性-稽核事件】

3.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。【中】【普】

行政院技服中心建議 107.11.15

進行Log之時機：

驗證成功與失敗、帳戶鎖定、密碼變更、敏感資料被讀取、資料異動及刪除、資料結構變更、管理者行為、查詢語法執行失敗、檔案存取錯誤、非預期的狀態

連線失敗、逾時及效能問題。

資通系統防護基準控制措施說明

【稽核與可歸責性-稽核事件】

4.應稽核資通系統管理者帳號所執行之各項功能。【中】【普】

【稽核與可歸責性-稽核紀錄內容】

2.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。

資通系統防護基準控制措施說明

【稽核與可歸責性-稽核紀錄內容】

1.資通系統產生之稽核紀錄，應依需求納入其他相關資訊。【中】

【稽核與可歸責性-稽核紀錄內容】

2.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。

資通系統防護基準控制措施說明

【稽核與可歸責性-稽核紀錄內容】【中】【普】

2.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。

行政院技服中心建議 107.11.15

1. 使用者ID紀錄不可為個資類型(如身分證號)
2. 系統日誌紀錄應盡可能採用單一的LOG機制，例如同一伺服器軟體應產出相同格式之日誌紀錄，以便於事件比對與追查

資通系統防護基準控制措施說明

【稽核與可歸責性-稽核儲存容量】

依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量。【中】【普】

資通系統防護基準控制措施說明

【稽核與可歸責性-稽核處理失效之回應】【中】【普】

資通系統於稽核處理失效時，應採取適當之行動。

資通系統防護基準控制措施說明

【稽核與可歸責性-時戳及校時】【中】

1.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。

資通系統防護基準控制措施說明

【稽核與可歸責性-時戳及校時】【中】【普】

2.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)

【稽核與可歸責性-稽核紀錄內容】

2.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。

資通系統防護基準控制措施說明

【稽核與可歸責性-稽核資訊之保護】

1.應運用雜湊或其他適當方式之完整性確保機制。

【中】

資通系統防護基準控制措施說明

【稽核與可歸責性-稽核資訊之保護】

2.對稽核紀錄之存取管理，僅限於有權限之使用者。【中】【普】

【稽核與可歸責性-稽核紀錄內容】

2.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。

資通系統防護基準控制措施說明

【營運持續計畫-系統備份】

1.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。 【中】

資通系統防護基準控制措施說明

【營運持續計畫-系統備份】

2.訂定系統可容忍資料損失之時間要求。【中】【普】

資通系統防護基準控制措施說明

【營運持續計畫-系統備份】

3.執行系統源碼與資料備份。【中】【普】

資通系統防護基準控制措施說明

【營運持續計畫-系統備援】【中】

1.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。

資通系統防護基準控制措施說明

【營運持續計畫-系統備援】【中】

2.原服務中斷時，於可容忍時間內，由備援設備取代提供服務。

資通系統防護基準控制措施說明

【識別與鑑別-內部使用者之識別與鑑別】 【中】【普】

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。

資通系統防護基準控制措施說明

【識別與鑑別-身分驗證管理】【中】

1.身分驗證機制應防範自動化程式之登入或密碼更換嘗試。

資通系統防護基準控制措施說明

【識別與鑑別-身分驗證管理】

2.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。【中】

資通系統防護基準控制措施說明

【識別與鑑別-身分驗證管理】

3.使用預設密碼入系統時，應於登入後要求立即變更。【中】【普】

資通系統防護基準控制措施說明

【識別與鑑別-身分驗證管理】

4.身分驗證相關資訊不以明文傳輸。 【中】【普】

資通系統防護基準控制措施說明

【識別與鑑別-身分驗證管理】

4.身分驗證相關資訊不以明文傳輸。

行政院技服中心建議 107.11.15

1. 避免採用不安全的協定(如SSL及TLS1.0版本)
2. 避免採用已被破解的加密演算法(如RC4、DES、3DES)

資通系統防護基準控制措施說明

【識別與鑑別-身分驗證管理】

5.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。【中】【普】

資通系統防護基準控制措施說明

【識別與鑑別-身分驗證管理】

5.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。

行政院技服中心建議 107.11.15

除鎖定帳號外亦可鎖定來源IP，以防範攻擊多個帳號，使同一來源無法再某個帳戶鎖定後，又再行嘗試攻擊其他帳號。

資通系統防護基準控制措施說明

【識別與鑑別-身分驗證管理】

6.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。【中】【普】

資通系統防護基準控制措施說明

【識別與鑑別-身分驗證管理】

7.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。【中】【普】

資通系統防護基準控制措施說明

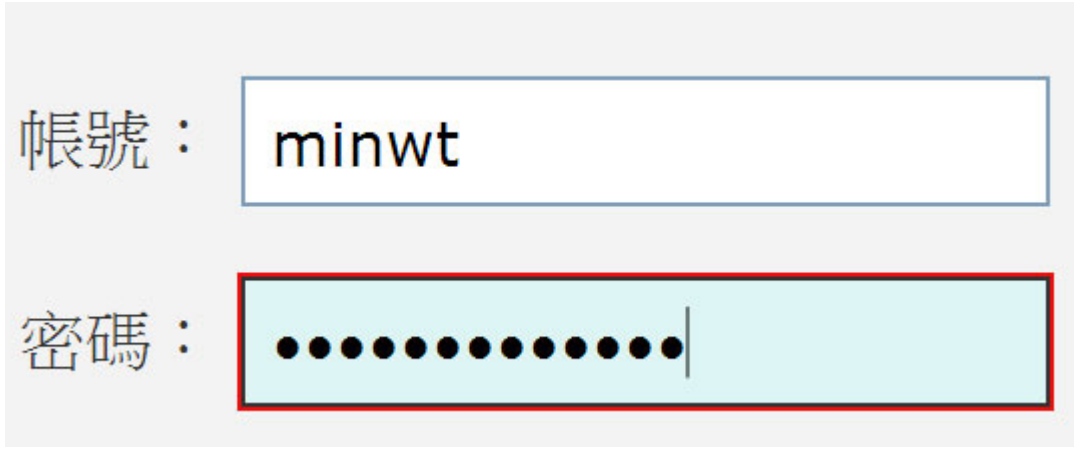
【識別與鑑別-身分驗證管理】

8.第六點及第七點所定措施，對非內部使用者，可依機關自行規範辦理。【中】【普】

資通系統防護基準控制措施說明

【識別與鑑別-鑑別資訊回饋】

資通系統應遮蔽鑑別過程中之資訊。【中】【普】



資通系統防護基準控制措施說明

【識別與鑑別-加密模組鑑別】

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。【中】

資通系統防護基準控制措施說明

【識別與鑑別-非內部使用者之識別與鑑別】

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)。【中】【普】

行政院技服中心建議 107.11.15

1. 資訊系統應識別使用者身分(如利用帳號)，並驗證使用者所宣稱之身分(如利用密碼)
2. 重要資訊系統(如管理者頁面)可限制來源IP位址(如僅限內部網路或本機)以強化安全性

資通系統防護基準控制措施說明

【系統與服務獲得-系統發展生命週期需求階段】

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。【中】【普】

資通系統防護基準控制措施說明

【系統與服務獲得-系統發展生命週期設計階段】

1.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。【中】

資通系統防護基準控制措施說明

【系統與服務獲得-系統發展生命週期設計階段】

2.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。【中】

資通系統防護基準控制措施說明

【系統與服務獲得-系統發展生命週期開發階段】

1.應針對安全需求實作必要控制措施。【中】【普】

資通系統防護基準控制措施說明

【系統與服務獲得-系統發展生命週期開發階段】

2.應注意避免軟體常見漏洞及實作必要控制措施。

【中】【普】

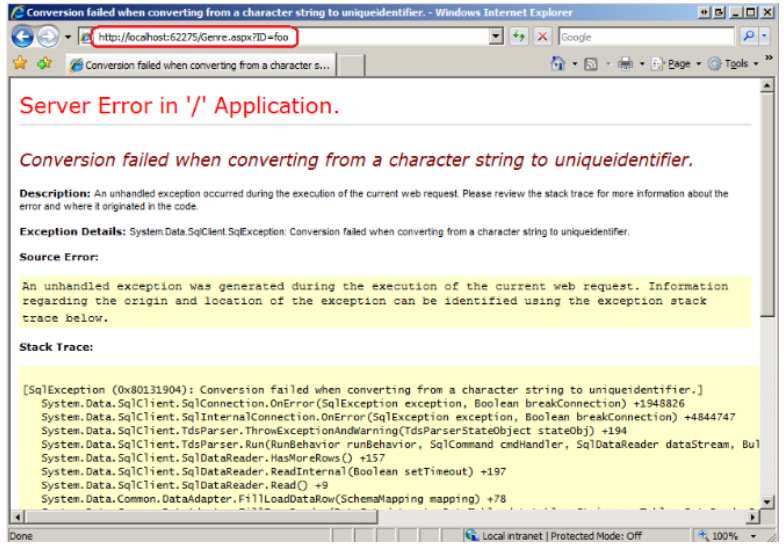
資通系統防護基準控制措施說明

【系統與服務獲得-系統發展生命週期開發階段】

3.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【中】【普】

行政院技服中心建議 107.11.15

發生錯誤時，頁面不應出現詳細的程式除錯訊息，避免攻擊者根據錯誤訊息刺探系統內部資訊或推測系統弱點。



資通系統防護基準控制措施說明

【系統與服務獲得-系統發展生命週期測試階段】

執行「弱點掃描」安全檢測。【中】【普】

資通安全責任等級分級辦法-B級之公務機關應辦事項

安全性檢測	網站安全弱點檢測	全部核心資通系統每年辦理一次。
	系統滲透測試	全部核心資通系統每二年辦理一次。

資通安全管理法施行細則-第四條

五、受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明；該資通系統屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測；涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

資通系統防護基準控制措施說明

【系統與服務獲得-系統發展生命週期部署與維運階段】

1.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。【中】【普】

資通系統防護基準控制措施說明

【系統與服務獲得-系統發展生命週期部署與維運階段】

2.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。【中】【普】

資通系統防護基準控制措施說明

【系統與服務獲得-系統發展生命週期部署與維運階段】

3.資通系統相關軟體，不使用預設密碼。【中】【普】

資通系統防護基準控制措施說明

【系統與服務獲得-系統發展生命週期委外階段】

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。【中】【普】

資通系統防護基準控制措施說明

【系統與服務獲得-獲得程序】

開發、測試及正式作業環境應為區隔。【中】

資通系統防護基準控制措施說明

【系統與服務獲得-系統文件】

應儲存與管理系統發展生命週期之相關文件。【中】【普】

資通系統防護基準控制措施說明

【系統與資訊完整性-漏洞修復】

1.定期確認資通系統相關漏洞修復之狀態。【中】

資通系統防護基準控制措施說明

【系統與資訊完整性-漏洞修復】

2.系統之漏洞修復應測試有效性及潛在影響，並定期更新。

【中】【普】

資通系統防護基準控制措施說明

【系統與資訊完整性-資通系統監控】

1.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。【中】

資通系統防護基準控制措施說明

【系統與資訊完整性-資通系統監控】

2.發現資通系統有被入侵跡象時，應通報機關特定人員。

【中】【普】

資通系統防護基準控制措施說明

【系統與資訊完整性-軟體及資訊完整性】

1.使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。

【中】

資通系統防護基準控制措施說明

【系統與資訊完整性-軟體及資訊完整性】

2.使用者輸入資料合法性檢查應置放於應用系統伺服器端。

【中】

資通系統防護基準控制措施說明

【系統與資訊完整性-軟體及資訊完整性】

3.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。【中】


Workshop

Thank You

感謝聆聽 敬請指教

陳泰龍 Felix

felix@bccs.com.tw