CipherTech
TRUST&SECURITY

資通安全管理法暨執行細則

對應解決方案

www.ciphertech.com.tw

資通安全管理法時程

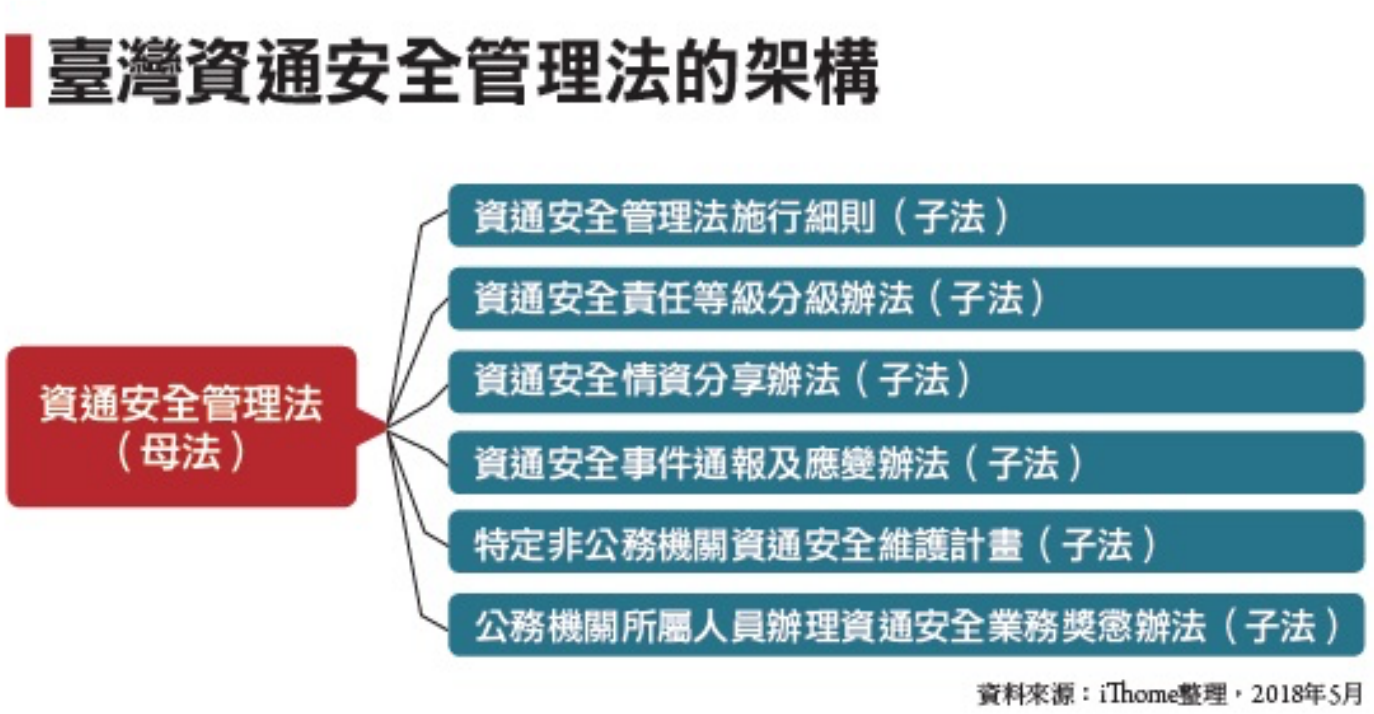
2017.04.27 – 行政院版資通安全管理法草案通過

2018.05.11 – 完成立法院三讀

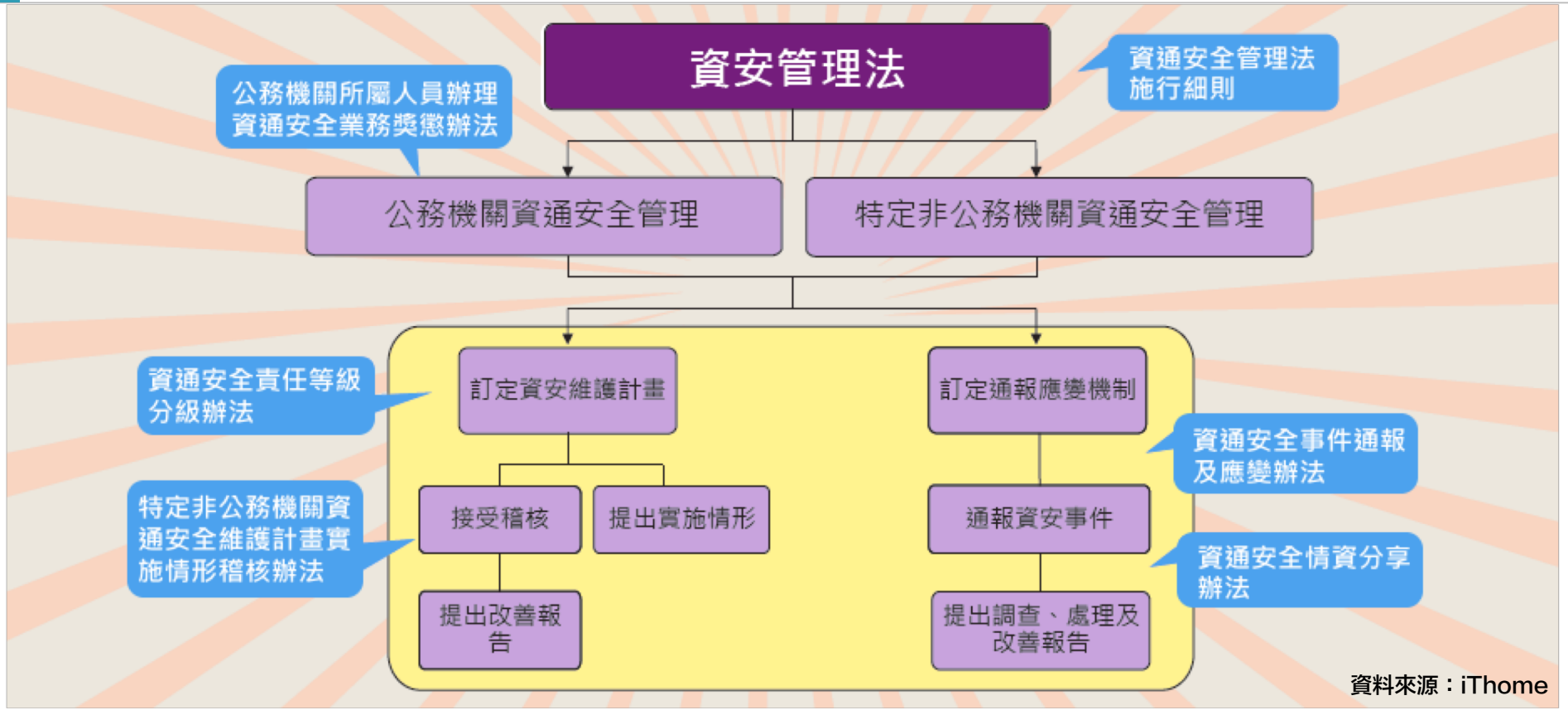
2018.06.06 – 總統府正式公佈

2019.01.01 – 正式施行

資通安全管理法架構(1/2)



資通安全管理法架構(2/2)



資通安全管理法適用對象

依據資通安全管理法第三條

公務機關

- 中央、地方機關(構)
- 公法人
- 不包括軍事及情報機關

特定非公務機關

- 關鍵基礎設施提供者
- 公營事業
- 政府捐助之財團法人

八大關鍵基礎設施領域	
能源	電力、石油、天然氣、化學與核能材料
水資源	水源、水庫、淨水系統、供水線路
通訊傳播	通訊、傳播
交通	陸運、海運、空運、氣象、郵政及物流
銀行與金融	銀行、證券、金融市場與外匯
緊急救援與醫院	緊急醫療部門、緊急應變體系
中央與地方政府機關	重要人員、重要場所設施、資訊與網路應用服務、重要文化資產與象徵
高科技園區	科學工業與生醫園區、軟體園區與工業區

罰則 - 公務機關

依據公務機關所屬人員資通安全事項獎懲辦法第四條,有下列情形之一者，予以懲處:

一、未依本法、本法授權訂定之法規或機關內部規 範辦理下列事項，情節重大:

(一)資通安全情資分享作業。

(二)訂定、修正及實施資通安全維護計畫。

(三)提出資通安全維護計畫實施情形。

(四)辦理資通安全維護計畫實施情形之稽核。

(五)配合上級或監督機關資通安全維護計畫實施情形稽核結果，提出改善報告。

(六)訂定資通安全事件通報及應變機制。

(七)資通安全事件之通報或應變作業。

(八)提出資通安全事件調查、處理及改善報告。

二、辦理資通安全業務經主管機關、上級或監督機 關評定績效不良，經疏導無效，情節重大。

三、其他違反本法、本法授權訂定之法規或機關內 部規範之行為，情節重大。

罰則 – 特定非公務機關

依據資通安全管理法第20條,限期改正，按次處新臺幣10萬～100萬罰鍰:	違反資安法第16條 違反資安法第17條 違反資安法第18-1, 18-3, 18-4條
依據資通安全管理法第21條,限期改正，按次處新臺幣30萬～500萬罰鍰:	未依18-2條規定，通報資通安全事件

資通安全責任等級之(非)公務機關應辦事項 – 管理面

辦理項目	辦理內容	A	B	C
資通系統分級及防護基準	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。	1年內	1年內	1年內 (系統等級為「高」者，2年內完成附表十之控制措施。)
資訊安全管理系統之導入及通過公正第三方之驗證	全部核心資通系統導入CNS27001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。	2年內	2年內	2年內 (不需第三方驗證)
資通安全專責人員	配置專職人員。	1年內 配置4人	1年內 配置2人	1年內 配置1人
業務持續運作演練	全部核心資通系統。	每年1次	每2年1次	每2年1次
內部資通安全稽核		每年2次	每年1次	每2年1次
資安治理成熟度評估(僅公務機關)		每年1次	每年1次	

資通安全責任等級之(非)公務機關應辦事項 – 技術面

辦理項目	辦理內容	A	B	C	D
安全性檢測	全部核心資通系統網站安全弱點檢測	每年2次	每年1次	每2年1次	
	全部核心資通系統滲透測試	每年1次	每2年1次	每2年1次	
資通安全健診	網路架構檢視	每年1次	每2年1次	每2年1次	
	網路惡意活動檢視				
	使用者端電腦惡意活動檢視				
	伺服器主機惡意活動檢視				
	目錄伺服器設定及防火牆連線設定檢視				
資通安全威脅偵測管理機制	完成威脅偵測機制建置，並持續維運。	1年內	1年內		
政府組態基準	初次受核定或等級變更後之一年內，依主管機關公告之項目，完成政府組態基準導入作業，並持續維運。	1年內	1年內		
資通安全防護 (完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級)	防毒軟體	1年內	1年內	1年內	1年內
	網路防火牆				
	具有郵件伺服器者，應備電子郵件過濾機制				
	入侵偵測及防禦機制				
	具有對外服務之核心通系統者，應備應用程式防火牆				
	進階持續性威脅攻擊防禦措施				

資通安全責任等級之(非)公務機關應辦事項 – 認知與訓練

辦理項目	辦理內容	A	B	C	D	E
資通安全教育訓練	資通安全及資訊人員 (每年接受資通安全專業課程訓練或資通安全職能訓練。)	4名 各12小時	2名 各12小時	1名 12小時		
	一般使用者及主管 (每人每年接受一般資通安全教育訓練。)	3小時	3小時	3小時	3小時	3小時
資通安全專業證照及職能訓練證書	資通安全專業證照 (一年內，資通安全專職人員總計應持有之證照，並持續維持證照之有效性。)	4張	2張	1張		
	資通安全職能評量證書(僅公務機關) (一年內，資通安全專職人員總計應持有之職能評量證書，並持續維持證書之有效性。)	4張	2張	1張		

資通系統防護需求分級原則

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。
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。
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。
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。

資通系統防護基準 - 控制措施1:存取控制

系統防護需求分級 措施內容	高	中	普
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。
遠端存取	一、應監控資通系統遠端連線。 二、資通系統應採用加密機制。 三、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。 四、等級「普」之所有控制措施。		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2:稽核與可歸責性

系統防護需求分級 措施內容	高	中	普
稽核事件	一、應定期審查稽核事件。 二、等級「普」之所有控制措施。		一、依規定時間週期及紀錄留存政策，保留稽核紀錄。 二、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。 三、應稽核資通系統管理者帳號所執行之各項功能。
稽核紀錄內容	一、資通系統產生之稽核紀錄，應依需求納入其他相關資訊。 二、等級「普」之所有控制措施。		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。
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。		
稽核處理失效之回應	一　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。 二　等級「中」及「普」之所有控制措施。	資通系統於稽核處理失效時，應採取適當之行動。	
時戳及校時	一、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。 二、等級「普」之所有控制措施。		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)。
稽核資訊之保護	一、定期備份稽核紀錄至與原稽核系統不同之實體系統。 二、等級「中」之所有控制措施。	一、應運用雜湊或其他適當方式之完整性確保機制。 二、等級「普」之所有控制措施。	對稽核紀錄之存取管理，僅限於有權限之使用者。

資通系統防護基準 - 控制措施3:營運持續計畫

系統防護需求分級 措施內容	高	中	普
系統備份	一、應將備份還原，作為營運持續計畫測試之一部分。 二、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。 三、等級「中」之所有控制措施。	一、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。 二、等級「普」之所有控制措施。	一、訂定系統可容忍資料損失之時間要求。 二、執行系統源碼與資料備份。
系統備援	一、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。 二、原服務中斷時，於可容忍時間內，由備援設備取代提供服務。		無要求。

資通系統防護基準 - 控制措施4:識別與鑑別

系統防護需求分級 措施內容	高	中	普
內部使用者之識別與鑑別	一、對帳號之網路或本機存取採取多重認證技術。 二、等級「中」及「普」之所有控制措施。	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。	
身分驗證管理	一、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 二、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。 三、等級「普」之所有控制措施。		一、使用預設密碼登入系統時，應於登入後要求立即變更。 二、身分驗證相關資訊不以明文傳輸。 三、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。 四、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。 五、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。 六、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。
鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊。		
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。		無要求。
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)。		

資通系統防護基準 - 控制措施5:系統與服務獲得

系統防護需求分級 措施內容	高	中	普
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。		
系統發展生命週期設計階段	一　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。 二、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。		無要求。
系統發展生命週期開發階段	一、執行「源碼掃描」安全檢測。 二、具備系統嚴重錯誤之通知機制。 三、等級「中」及「普」之所有控制措施。	一、應針對安全需求實作必要控制措施。 二、應注意避免軟體常見漏洞及實作必要控制措施。 三、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。	
系統發展生命週期測試階段	一、執行「滲透測試」安全檢測。 二、等級「中」及「普」之所有控制措施。	執行「弱點掃描」安全檢測。	
系統發展生命週期部署與維運階段	一、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。 二、等級「普」之所有控制措施。		一、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。 二、資通系統相關軟體，不使用預設密碼。
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。		
獲得程序	開發、測試及正式作業環境應為區隔。		無要求。
系統文件	應儲存與管理系統發展生命週期之相關文件。		

資通系統防護基準 - 控制措施6:系統與通訊保護

系統防護需求分級 措施內容	高	中	普
傳輸之機密性與完整性	一、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。 二、使用公開、國際機構驗證且未遭破解之演算法。 三、支援演算法最大長度金鑰。 四、加密金鑰或憑證週期性更換。 五、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。	無要求。	無要求。
資料儲存之安全	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。	無要求。

資通系統防護基準 - 控制措施7:系統與資訊完整性

系統防護需求分級 措施內容	高	中	普
漏洞修復	一、定期確認資通系統相關漏洞修復之狀態。 二、等級「普」之所有控制措施。		系統之漏洞修復應測試有效性及潛在影響，並定期更新。
資通系統監控	一、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。 二、等級「中」之所有控制措施。	一、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。 二、等級「普」之所有控制措施。	發現資通系統有被入侵跡象時，應通報機關特定人員。
軟體及資訊完整性	一、應定期執行軟體與資訊完整性檢查。 二、等級「中」之所有控制措施。	一、使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。 二、使用者輸入資料合法性檢查應置放於應用系統伺服器端。 三、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。	無要求。

產品對應

控制措施	內容	解決方案	產品名稱
存取控制	帳號管理	特權維運管理系統	CPS UAP新一代維運稽核與風險控制系統
	最小權限	特權維運管理系統	CPS UAP新一代維運稽核與風險控制系統
	遠端存取	特權維運管理系統	CPS UAP新一代維運稽核與風險控制系統
稽核與可歸責性	稽核事件	資料庫稽核系統	iMPERVA DAM
	稽核紀錄內容	資料庫稽核系統	iMPERVA DAM
	稽核儲存容量	資料庫稽核系統	iMPERVA DAM
	稽核處理失效之回應	資料庫稽核系統	iMPERVA DAM
	時戳及校時	資料庫稽核系統	iMPERVA DAM
	稽核資訊之保護	資料庫稽核系統	iMPERVA DAM
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	特權維運管理系統	CPS UAP新一代維運稽核與風險控制系統
	身份驗證管理	特權維運管理系統	CPS UAP新一代維運稽核與風險控制系統
	鑑別資訊回饋	資料去識別化	Vormetric DSM+VTS
	加密模組鑑別	資料去識別化	Vormetric DSM+VTS
	非內部使用者之識別與鑑別		

CipherTech TRUST&SECURITY

產品對應

控制措施	內容	解決方案	產品名稱
系統與服務獲得	系統發展生命週期需求階段		
	系統發展生命週期設計階段		
	系統發展生命週期開發階段		
	系統發展生命週期測試階段	弱點掃描系統	中華龍網弱點掃描系統
	系統發展生命週期部署與維運階段		
	系統發展生命週期委外階段		
	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	資料保護解決方案	Vormetric DSM/VTE/VTS/金鑰管理
	資料儲存之安全	資料保護解決方案	Vormetric DSM/VTE/VTS/金鑰管理
系統與資訊完整性	漏洞修復		
	資通系統監控	網站應用程式防火牆	iMPERVA WAF
		資料庫稽核	iMPERVA DAM
	軟體及資訊完整性	程式碼簽章	Code Sign