資通安全管理制度內部稽核表					
文件編號	TKMS-ISMS-D-039	機密等級	限閱	版次	1.0

紀錄編號：　　填表日期：　　年　　月　　日

評分標準說明：

A：相關資訊安全管理制度規範已建立，且落實執行

B：相關資訊安全管理制度規範未建立，但已實施替代性資安控管措施

C：相關資訊安全管理制度規範已建立，但未落實執行

D：相關資訊安全管理制度規範未建立，且未實施替代性資安控管措施

E：不適用

條款 章節	條文	稽核評分					稽核發現說明
		A	B	C	D	E	
陸、	適用性聲明(Statement of Applicability)						
	ISMS 施行單位可依據適用單位等級選擇控制措施，參考附錄 A 之控制措施，產生「ISMS 適用性聲明」。各等級單位適用之控制措施請參照「附錄 A 資訊安全管理規範 附件 1 各級教育機構適用控制項對照表」。附錄 A 控制措施之排除僅限適用範圍內資訊系統無需執行，且排除後不影響該單位提供資通安全能力與責任之控制措施。 教育機構如欲取得驗證，所有附錄 A 資訊安全管理規範內之控制項，除標註「建議」者外均應納入，同時應參考「資訊系統分級與資安防護基準作業規	☐	☐	☐	☐	☐	

	定」，鑑別適用範圍內資訊系統之安全等級，經資訊系統分級與鑑別後，識別出具有等級為「高」者之資訊系統，應加入 A.14 系統獲取、開發及維護與 A.15 供應者關係等控制領域所有控制措施，並於該控制措施中述明適用之資訊系統。		
柒、	建置步驟及需求		
一、	組織全景		
	(一)施行單位應依據行政管理會議(如主管會報、行政會議或校務會議等)中有關資通訊或個人資訊管理需求決議事項進行評估，並據此建立或調整資通訊安全與個人資訊管理範圍與目標。	□ □ □ □ □	
	(二)施行單位應依據決議事項確認其利害相關團體與要求事項，並留存文件化紀錄。	□ □ □ □ □	
	(三)上述事項之識別與分析應定期審查(每年至少一次)，或於施行單位遭遇重大變更、新業務時重新檢視，並供管理審查時評估管理系統及其適用範圍調整必要性。	□ □ □ □ □	
二、	領導作為		
	(一)領導及承諾 施行單位應由副首長擔任或指定管理制度之管理人或召集人，並藉由下列事項，展現對管理制度之領導與承諾： 1.建立或核定施行單位之管理政策與目標。	□ □ □ □ □	

	2.傳達管理制度要求事項之遵循與持續改善的承諾。 3.提供管理制度運行所需資源及人力。							
	(二)建立政策與目標 管理人或召集人應確保建立文件化的管理政策，並於施行單位內進行公告或傳達，同時依需要提供予利害相關團體。	☐	☐	☐	☐	☐		
	管理政策應包含符合施行單位之管理目的與目標與滿足管理制度要求事項與持續改善的承諾。	☐	☐	☐	☐	☐		
	施行單位應依規劃期間或重大變更時，於透過管理審查管理活動評估管理政策與目標，並配合變更需求修訂政策與目標。	☐	☐	☐	☐	☐		
	(三)單位角色、責任及權限 管理人或召集人應建立制度管理小組，依施行單位特性，指派人員並賦予其管理之責任與權限，以促進達成本規範之要求事項。	☐	☐	☐	☐	☐		
	受指派人員應定期（每年至少一次）或於重大變更時向管理階層報告管理制度執行成效。ISMS 與 PIMS 所配置人員應依據附錄 A.6 資訊安全組織與附錄 B.2 個人資料管理組織派任。	☐	☐	☐	☐	☐		
三、	規劃							
	(一)管理目標達成風險與機會之因應行動 為確保達成制度管理目標，並預防或減少非預期之影響，以達成持續改善，應於應依規劃期間或重大	☐	☐	☐	☐	☐		

	變更時，評估管理目標異動與達成情形，如有異動或未達成狀況，則應規劃因應風險與機會之行動，將各項行動整合及實作於管理制度中，並評估此行動之有效性。 PIMS 並應依附錄 B.4 個人資料之識別與風險管理要求執行。							
	(二)建立風險管理程序 應參考「資訊系統分級與資安防護基準作業規定」，鑑別適用範圍內資訊系統之安全等級，其安全等級應採鑑別結果最高者，應執行風險評鑑與處理流程。	☐	☐	☐	☐	☐		
	風險評鑑與處理流程建立應符合下列要求事項： 1.建立與維持風險準則 包含風險評鑑執行時機與方法，以及風險接受準則，以確保重複之風險評鑑能產生一致、有效及可比較之結果。	☐	☐	☐	☐	☐		
	2.識別、分析並評估風險 識別管理制度適用範圍內涉及資訊洩漏之機密性、完整性、可用性與適法性相關聯之風險與風險擁有者。 所識別之風險可能導致之潛在後果與發生的實際可能性，並將所建立之風險準則與風險分析結果進行比較，訂定風險處理優先順序。	☐	☐	☐	☐	☐		
	3.選擇風險處理措施	☐	☐	☐	☐	☐		

	考量風險評鑑結果，選擇適切之風險處理選項，並依選項決定所有必須實作之控制措施；		
	4.產生或評估適用性聲明書(資訊安全風險處理使用) 執行資訊安全風險評鑑時，應依據資訊資產分級結果重現檢視比較現有控制措施及附錄 A，確認未忽略必要之控制措施，並產生或評估適用性聲明書，包括必要之控制措施，且不論是否實作，提供納入或排除之理由；	☐ ☐ ☐ ☐ ☐	
	5.制訂風險處理計畫並取得核准 制訂風險處理計畫，並取得風險擁有者對風險處理計畫之核准，以及對剩餘風險之接受。	☐ ☐ ☐ ☐ ☐	
	(三)管理目標及其達成之規劃 施行單位應針對異動與未達成之管理目標，設定符合管理政策與策略之可量測指標，並保存保存管理目標之文件化資訊。	☐ ☐ ☐ ☐ ☐	
	施行單位應對前述管理目標規劃因應行動，包含： 1.相關執行活動或事項； 2.所需投入之人員、預算、設備技術與程序表單等資源； 3.活動或事項負責人員； 4.活動或事項預計完成時間； 5.管理目標是否達成之評估方式。	☐ ☐ ☐ ☐ ☐	
四、	支援		

	(一)資源 施行單位應依據管理目標達成規劃，提供建立、實行、維持及持續改善管理制度所需資源。	☐	☐	☐	☐	☐	
	(二)能力 施行單位應採取下列措施： 1.僅指派受過適當教育訓練、具備證照或具有經驗人員，執行資通安全或個人資料管理相關任務；規劃培訓以強化人員能力時，應評估培訓之有效性。	☐	☐	☐	☐	☐	
	2.有關人員能力訓練，ISMS 應參照附錄 A.7 人力資源安全，PIMS 則依附錄 B.3 人員認知與訓練要求執行。	☐	☐	☐	☐	☐	
	3.應保存文件化資訊(如：如證書、證照、培訓紀錄等)，作為人員勝任之證據。	☐	☐	☐	☐	☐	
	(三)認知 應規劃人員認知宣導或訓練，讓所有人員知悉： 1.管理政策及目標， 2.管理程序與流程要求事項與人員責任， 3.未遵循要求可能產生對個人與單位的影響與衝擊，其包含但不限於懲處。	☐	☐	☐	☐	☐	
	ISMS 應參照附錄 A.7 人力資源安全，PIMS 則依附錄 B.3 人員認知與訓練要求進行說明。	☐	☐	☐	☐	☐	
	(四)文件化資訊 管理制度文件化資訊應滿足下列要求：	☐	☐	☐	☐	☐	

	1.施行單位之管理制度文件應包括本規範要求之文件化資訊,及施行單位要求管理制度為達成其有效性之文件化資訊與作業紀錄。						
	2.制訂及更新應遵循既有文件管理程序，進行審查及核准。	☐	☐	☐	☐	☐	
	3.管控文件化資訊派送、存取、檢索、使用、儲存與保存、變更管制、留存及屆期處置,並適切保護。	☐	☐	☐	☐	☐	
	4.施行單位應識別對管理制度規劃及運作必要之外部文件。	☐	☐	☐	☐	☐	
五、	運作						
	(一)運作之規劃及控制 施行單位之管理制度運作應滿足下列要求： 1.應依據管理制度各階文件，以及為達成管理目標所規劃之流程、程序與控制措施執行，並應保存保存執行證據。	☐	☐	☐	☐	☐	
	2.ISMS 應依據所屬級別實作選定之附錄 A 控制措施，PIMS 則應實作附錄 B 訂定之控制措施。	☐	☐	☐	☐	☐	
	3.應確保各項委外執行作業受到控制與管理，屬 ISMS 委外管理可連結附錄 A.15 供應者管理，PIMS 則依據附錄 B.12 委外管理執行。	☐	☐	☐	☐	☐	
	(二)執行風險評鑑 1.施行單位依規劃期間(至少每年一次)、管理階層指示或發生重大變更後一個月內,應執行風險評鑑，確認管理制度各項風險加以識別，並保存	☐	☐	☐	☐	☐	

	風險評鑑執行紀錄；							
	2.PIMS 施行單位應分析可能造成當事人損失或困擾之個人資訊處理流程，由風險擁有者進行審查；	☐	☐	☐	☐	☐		
	3.擬定風險處理計畫，並取得風險擁有者對其及剩餘風險之核准。	☐	☐	☐	☐	☐		
	(三)實作風險處理 施行單位應實作風險處理計畫並保存風險處理結果之文件化證據資訊。	☐	☐	☐	☐	☐		
六、	績效評估							
	(一)監督、量測、分析及評估 1.施行單位應針對已施行之常態性作業流程或控制措施建立監督機制，如機房管理、網路管理作業審查等。	☐	☐	☐	☐	☐		
	2.對於本次異動管理目標，以及風險處理措施設定有效性量測指標，並界定明確計算方式與資料來源、量測人員、週期與時間點，以及分析及評估量測結果之人員、週期與時間點。	☐	☐	☐	☐	☐		
	3.應留存文件化資訊，作為有效性評估證據。	☐	☐	☐	☐	☐		
	(二)內部稽核 1.施行單位應定期(至少每年一次)執行一次內部稽核，以確認單位與人員是否遵循本規範與單位管理程序要求，並有效實作及維持管理制度。	☐	☐	☐	☐	☐		

	ISMS 施行單位可連結附錄 A.18 遵循性執行。		
	2.稽核程序應包括頻率、方法、職責、規劃要求事項及報告。稽核計畫應包含適用範圍內核心業務與高風險個人資料流程或系統，並將前次稽核之結果納入考量。	□ □ □ □ □	
	3.稽核員應受適當培訓並具備稽核能力，且不得稽核自身經辦業務，以確保稽核過程之客觀性及公平性。	□ □ □ □ □	
	4.稽核結果應對相關管理階層報告，留存相關紀錄以作為稽核計畫及稽核結果之證據。	□ □ □ □ □	
	(三)管理審查 管理小組應定期(每年至少一次)進行管理審查，以審查管理制度執行狀況，並確保其持續的適切性、合宜性及有效性。	□ □ □ □ □	
	1.管理審查應包含下列討論事項： (1)過往管理審查之議案的處理狀態； (2)資通訊安全或個資管理要求的變更，如上級機關要求、最高行政管理會議決議事項； (3)管理目標與指標量測結果 (4)內外部稽核結果； (5)資安事故與不符合項目之矯正情形 (6)風險評鑑結果及風險處理計畫執行進度； (7)持續改善之機會。	□ □ □ □ □	

	2.管理審查決議事項應包含持續改善機會與管理制度變更需求之決議。	☐	☐	☐	☐	☐	
	3.施行單位應保存相關紀錄，以作為管理審查執行之證據。	☐	☐	☐	☐	☐	
七、	改善						
	(一)不符合項目及矯正措施 不符合項目發生時，施行單位應進行下列作為，並保存紀錄： 1.先對不符合項目採取行動以控制並矯正，進而處理其後果。	☐	☐	☐	☐	☐	
	2.判定其發生原因及矯正措施，並評估是否有其類似不符合項目存在，並據此提出並執行矯正措施，並必要時得考量對管理制度進行變更。	☐	☐	☐	☐	☐	
	(二)持續改善 施行單位應持續改善管理制度的合宜性、適切性及有效性。	☐	☐	☐	☐	☐	

稽核項目 – 控制目標與控制項目

控制項	條文		稽核評分					稽核發現說明
			A	B	C	D	E	
A5	資訊安全政策							
A.5.1	資訊安全之管理指導方針							
A.5.1.1 (I/P)	資訊安全政策	資訊安全政策應由管理階層定義並核准，且對給所有員工及相關外部各方公布及傳達。	☐	☐	☐	☐	☐	
A.5.1.2 (I/P)	資訊安全政策之審查	資訊安全政策應依規劃之期間或發生重大變更時審查，以確保其持續的合宜性、適切性及有效性。	☐	☐	☐	☐	☐	
A6	資訊安全組織							
A.6.1	內部組織							
A.6.1.1 (I/P)	資訊安全之角色及責任	應定義及配置所有資訊安全責任。	☐	☐	☐	☐	☐	
A.6.1.2	職務區隔	衝突之職務及責任範圍應予以區隔，以降低組織資產遭未經授權或非蓄意修改或誤用之機會。	☐	☐	☐	☐	☐	
A.6.1.3	與權責機關之聯繫	應維持與相關權責機關之適切聯繫。	☐	☐	☐	☐	☐	
A.6.1.4	與特殊關注方之聯繫	應維持與各特殊關注方或其他各種專家安全論壇及專業協會之適切聯繫。	☐	☐	☐	☐	☐	

控制項	條文		稽核評分					稽核發現說明
			A	B	C	D	E	
A.6.1.5 (建議)	專案管理之資訊安全	不論專案之型式，應在專案管理中因應資訊安全。	☐	☐	☐	☐	☐	
A.6.2	行動裝置及遠距工作							
A.6.2.1	行動裝置政策	應採用政策及支援之安全措施，以管理因使用行動裝置所導致之風險。	☐	☐	☐	☐	☐	
A.6.2.2	遠距工作	應實作政策及支援之安全措施，以保護存取、處理或儲存於遠距工作場所之資訊。	☐	☐	☐	☐	☐	
A.7	人力資源安全							
A.7.1	聘用前							
A.7.1.1 (I/P)	篩選	對所有可能被聘用者所進行之背景調查，應依照相關法律、法規及倫理， 並應相稱於營運要求及其將存取之資訊保密等級及組織所察覺之風險聘用。	☐	☐	☐	☐	☐	
A.7.1.2 (I/P)	聘用條款及條件	施行單位與員工及承包者簽訂之契約化協議書，應敘明雙方對資訊安全的責任。	☐	☐	☐	☐	☐	
A.7.2	聘用期間							
A.7.2.1 (I/P)	管理階層責任	管理階層應要求所有員工及承包者，依施行單位所建立政策及程序施行資訊安全事宜。	☐	☐	☐	☐	☐	

控制項	條文		稽核評分					稽核發現說明
			A	B	C	D	E	
A.7.2.2 (I/P)	資訊安全認知、教育及訓練	施行單位內所有員工及相關之承包者，均應接受及其工作職務相關的組織政策及程序之適切認知、教育及訓練，並定期更新。	☐	☐	☐	☐	☐	
A.7.2.3	懲處過程	應具備正式即已傳達之懲處過程，以對違反資訊安全之員工採取行動。	☐	☐	☐	☐	☐	
A.7.3	聘用之終止及變更							
A.7.3.1 (I/P)	聘用責任之終止或變更	應對員工及承包者定義、傳達於聘用終止或變更後資訊安全責任及義務仍保持有效，並執行之。	☐	☐	☐	☐	☐	
A.8	資產管理							
A.8.1	資產責任							
A.8.1.1 (I/P)	資產清冊	應識別與資訊及資訊處理設施相關聯之資產，並製作及維持此等資產之清冊。	☐	☐	☐	☐	☐	
A.8.1.2	資產擁有權	清冊中所維持之資產應有擁有者。	☐	☐	☐	☐	☐	
A.8.1.3	資產之可被接受的使用	對與資訊及資訊處理設施相關聯之資訊及資產，應識別、文件化及實作可被接受使用之規則。	☐	☐	☐	☐	☐	

控制項	條文		稽核評分					稽核發現說明
			A	B	C	D	E	
A.8.1.4	資產之歸還	所有員工及外部使用者於其聘用、契約或協議終止時，應歸還其據有之全部組織資產。	☐	☐	☐	☐	☐	
A.8.2	資訊分級							
A.8.2.1 (I/P)	資訊之分級	資訊應依法律要求、價值、重要性及其對未經授權揭露或修改之敏感性分級。	☐	☐	☐	☐	☐	
A.8.2.2 (I/P)	資訊之標示	應依施行單位所採用之資訊級方案，發展及實作一套適切的資訊標示程序。	☐	☐	☐	☐	☐	
A.8.2.3 (I/P)	資產之處置	應依施行單位所採用之資訊分級方案， 發展及實作處置資產之程序。	☐	☐	☐	☐	☐	
A.8.3	媒體處理							
A.8.3.1 (I/P)	可移除式媒體之管理	應依施行單位所採用之資訊分級方案， 實作管理可移除式媒體之程序。	☐	☐	☐	☐	☐	
A.8.3.2 (I/P)	媒體之汰除	當不再需要媒體時，應使用正式程序加以安全汰除。	☐	☐	☐	☐	☐	
A.8.3.3 (I/P)	實體媒體傳送	應保護含有資訊之媒體在傳送時，不受未經授權的存取、誤用或毀損。	☐	☐	☐	☐	☐	
A.9	存取控制							
A.9.1	存取控制之營運要求事項							

控制項	條文		稽核評分					稽核發現說明
			A	B	C	D	E	
A.9.1.1 (I/P)	存取控制政策	存取控制政策應依據營運及資訊安全要求事項，建立、文件化及審查之。	☐	☐	☐	☐	☐	
A.9.1.2	對網路及網路服務之存取	應僅提供予使用者存取其已被特定授權使用之網路及網路服務。	☐	☐	☐	☐	☐	
A.9.2	使用者存取管理							
A.9.2.1 (I/P)	使用者註冊與註銷	應實作正式之使用者註冊及註銷過程， 俾能指派存取權限。	☐	☐	☐	☐	☐	
A.9.2.2 (I/P) (建議)	使用者存取權限之配置	應實作正式之使用者存取權限配置程序，以對所有型式之使用者對所有系統及服務，指派或撤銷存取權限。	☐	☐	☐	☐	☐	
A.9.2.3 (I/P)	具特殊存取權限之管理	應限制及控制具特殊存取權限之配置及使用。	☐	☐	☐	☐	☐	
A.9.2.4 (I/P)	使用者之秘密鑑別資訊的管理	應以正式之管理過程控制秘密鑑別資訊的配置。	☐	☐	☐	☐	☐	
A.9.2.5 (I/P)	使用者存取權限之審查	施行單位應定期審查使用者存取權限。	☐	☐	☐	☐	☐	

控制項	條文		稽核評分					稽核發現說明
			A	B	C	D	E	
A.9.2.6 (I/P)	存取權限之移除或調整	所有員工及外部使用者對資訊及資訊處理設施之存取權限， 一旦其聘用、契約或協議終止時，均應予以移除；或於其聘用、契約或協議變更時均須調整之。	☐	☐	☐	☐	☐	
A.9.3	使用者責任							
A.9.3.1 (I/P)	秘密鑑別資訊之使用	於使用秘密鑑別資訊時，應要求使用者遵循施行單位之實務規定。	☐	☐	☐	☐	☐	
A.9.4	系統及應用存取控制							
A.9.4.1 (I/P)	資訊存取限制	應根據存取控制政策， 限制對資訊及應用系統功能之存取。	☐	☐	☐	☐	☐	
A.9.4.2 (I/P)	保全登入程序	當存取控制政策要求時，應以保全登入程序，控制對系統及應用之存取。	☐	☐	☐	☐	☐	
A.9.4.3 (I/P)	通行碼管理系統	通行碼管理系統應為互動式， 並應確保嚴謹通行碼。	☐	☐	☐	☐	☐	
A.9.4.4	具特殊權限公用程式之使用	應限制及嚴密控制可能篡越系統及應用控制措施之公用程式的使用。	☐	☐	☐	☐	☐	
A.9.4.5	對程式源碼之存取控制	應限制對程式原始碼之存取。	☐	☐	☐	☐	☐	
A.10	密碼學(加密控制)							

控制項	條文		稽核評分					稽核發現說明
			A	B	C	D	E	
A.10.1	密碼式控制措施(加密控制措施)							
A.10.1.1 (I/P)	使用密碼式控制措施(加密控制措施)政策	應發展及實作政策，關於資訊保護之密碼式控制措施的使用。	☐	☐	☐	☐	☐	
A.10.1.2 (建議)	金鑰管理	應加以發展及實作政策，關於貫穿其整個生命週期之密碼金鑰的使用、保護及生命期。	☐	☐	☐	☐	☐	
A.11	實體及環境安全							
A11.1	安全區域							
A11.1.1 (I/P)	實體安全周界	應定義及使用安全周界，以保護收容敏感或重要資訊及資訊處理設施之區域。	☐	☐	☐	☐	☐	
A.11.1.2 (I/P)	實體進入控制措施	保全區域應藉由適切之進入控制措施加以保護，以確保僅允許經授權人員進出。	☐	☐	☐	☐	☐	
A.11.1.3	保全之辦公室、房間及設施	應設計資訊處理設施所在區域之實體安全並施行之。	☐	☐	☐	☐	☐	
A.11.1.4	防範外部及環境威脅	應設計並施行實體保護，以防範天然災害、惡意攻擊或事故。	☐	☐	☐	☐	☐	

控制項	條文		稽核評分					稽核發現說明
			A	B	C	D	E	
A.11.1.5	於保全區域內工作	應設計及施行資訊處理設施所在區域內工作之程序。	☐	☐	☐	☐	☐	
A.11.1.6 (建議)	交付及裝卸區	對諸如交付及裝卸區及其他未經授權人員可進入作業場所之進出點，應加以控制；若可能，應與資訊處理設施隔離，以避免未經授權之存取。	☐	☐	☐	☐	☐	
A.11.2	設備							
A.11.2.1 (I/P)	設備安置及保護	應安置並保護設備， 以降低來自環境之威脅及危害造成的風險， 以及未經授權存取之機會。	☐	☐	☐	☐	☐	
A.11.2.2	支援之公用服務事業	應保護設備免於電源失效，及因其他支援之公用服務事業失效，所導致之中斷。	☐	☐	☐	☐	☐	
A.11.2.3	佈纜安全	應保護通訊纜線及資訊處理設備之電源，降低受竊聽或破壞的可能損失。	☐	☐	☐	☐	☐	
A.11.2.4 (I/P)	設備維護	應正確維護設備， 以確保其持續之可用性及完整性。	☐	☐	☐	☐	☐	
A.11.2.5 (I/P)	財產之攜出	未經事前授權，不得將設備、資訊或軟體帶出場域外。	☐	☐	☐	☐	☐	

控制項	條文		稽核評分					稽核發現說明
			A	B	C	D	E	
A.11.2.6 (建議)	場所外設備及資產的安全	安全應適用於場域外資產，並將於施行單位場所外工作之不同風險納入考量。	☐	☐	☐	☐	☐	
A.11.2.7 (I/P)	設備汰除或再使用之保全	含有儲存媒體之所有設備組件， 於汰除前或再使用前應加以查證，以確保任何敏感性資料及有版權之軟體已被移除或安全地覆寫。	☐	☐	☐	☐	☐	
A.11.2.8 (建議)	無人看管之使用者設備	使用者應確保無人看管之設備具備適切保護。	☐	☐	☐	☐	☐	
A.11.2.9	桌面淨空及螢幕淨空政策	對紙本及可移除式儲存媒體應採用桌面淨空政策， 且對資訊處理設施應採用螢幕淨空政策。	☐	☐	☐	☐	☐	
A.12	運作安全							
A.12.1	運作程序及責任							
A.12.1.1	文件化運作程序	運作程序應加以文件化， 並使所有需要之使用者均可取得。	☐	☐	☐	☐	☐	
A.12.1.2 (I/P)	變更管理	應控制對影響資訊安全之組織、營運過程、資訊處理設施及系統的變更。	☐	☐	☐	☐	☐	
A.12.1.3	容量管理	各項資源之使用應受監視及調適，並對未來容量要求預作規劃， 以確保所要求之系統效能。	☐	☐	☐	☐	☐	

控制項	條文		稽核評分					稽核發現說明
			A	B	C	D	E	
A.12.1.4	開發、測試及運作環境之區隔	應區隔開發、測試及運作之環境， 以降低對運作環境未經授權存取或變更的風險。	☐	☐	☐	☐	☐	
A.12.2	防範惡意軟體							
A.12.2.1 (I/P)	防範惡意軟體之控制措施	應實作防範惡意軟體之偵測、預防及復原控制措施，並合併適切之使用者認知。	☐	☐	☐	☐	☐	
A.12.3	備份							
A.12.3.1 (I/P)	資訊備份	應依議定之備份政策，定期取得資訊、軟體及系統的影像檔備份複本，並測試之。	☐	☐	☐	☐	☐	
A.12.4	存錄及監視							
A.12.4.1 (I/P)	事件存錄	應產生、保存並定期審查記錄使用者活動、異常、錯誤及資訊安全事件之事件日誌。	☐	☐	☐	☐	☐	
A.12.4.2 (I/P)	日誌資訊之保護	應防範存錄設施及日誌資訊遭竄改及未經授權存取。	☐	☐	☐	☐	☐	
A.12.4.3 (I/P)	管理者及操作者日誌	應存錄系統管理者及操作者之活動，且應保護及定期審查該日誌。	☐	☐	☐	☐	☐	

控制項	條文		稽核評分					稽核發現說明
			A	B	C	D	E	
A.12.4.4	鐘訊同步	組織或安全領域內所有相關資訊處理系統之鐘訊， 應與單一參考時間源同步。	☐	☐	☐	☐	☐	
A.12.5	運作中軟體之控制							
A.12.5.1	運作中系統之軟體安裝	應實作各項程序，以控制對運作中系統之軟體安裝。	☐	☐	☐	☐	☐	
A.12.6	技術脆弱性管理							
A.12.6.1	技術脆弱性管理	應及時取得關於使用中之資訊系統的技術脆弱性資訊、並應評估組織對此等脆弱性之暴露， 且應採取適當措施以因應相關風險。	☐	☐	☐	☐	☐	
A.12.6.2 (建議)	對軟體安裝之限制	應建立並實作使用者安裝軟體之管控規則。	☐	☐	☐	☐	☐	
A.12.7	資訊系統稽核考量							
A.12.7.1	資訊系統稽核控制措施	應仔細規劃並議定，涉及運作中系統之稽核要求事項及活動，以使營運過程中斷降至最低。	☐	☐	☐	☐	☐	
A. 13	通訊安全							
A.13.1	網路安全管理							
A.13.1.1	網路控制措施	應實施網路控制措施，維護網路安全。	☐	☐	☐	☐	☐	

控制項	條文		稽核評分					稽核發現說明
			A	B	C	D	E	
A.13.1.2	網路服務之安全	應識別所有網路服務之安全機制、服務等級及管理要求事項，並應被納入網路服務協議中，不論此等服務係由內部或委外所提供。	☐	☐	☐	☐	☐	
A.13.1.3	網路之區隔	應區隔各群組之資訊服務、使用者及資訊系統使用的網路。	☐	☐	☐	☐	☐	
A.13.2								
A.13.2.1 (I/P)	資訊傳送政策及程序	應備妥正式之傳送政策、程序及控制措施，以保護經由使用所有型式通訊設施之資訊傳送。	☐	☐	☐	☐	☐	
A.13.2.2 (I/P)	資訊傳送協議	協議應闡明組織與外部各方間營運資訊之安全傳送。	☐	☐	☐	☐	☐	
A.13.2.3 (I/P)	電子傳訊	應適切保護電子傳訊時所涉及之資訊。	☐	☐	☐	☐	☐	
A.13.2.4 (I/P)	機密性或保密協議	應識別、定期審查及文件化，以反映施行單位對資訊保護之需要的機密性或保密協議之要求事項。	☐	☐	☐	☐	☐	
A. 14	系統獲取、開發及維護							
A.14.1	資訊系統之安全要求事項							

控制項	條文		稽核評分					稽核發現說明
			A	B	C	D	E	
A.14.1.1 (I/P)	資訊安全要求事項分析及規格	資訊安全相關要求，應納入新資訊系統或既有資訊系統之強化的要求事項中。	☐	☐	☐	☐	☐	
A.14.1.2	保全公共網路之應用服務	應防範於公共網路上傳送的應用服務中涉及之資訊，免於詐欺活動、契約爭議及未經授權揭露與修改。	☐	☐	☐	☐	☐	
A.14.1.3 (建議)	保護應用服務交易	應保護應用服務交易中涉及之資訊，以防止不完整的傳輸、誤選路（mis-routing），未經授權之訊息修改、未經授權之揭露、未經授權之訊息複製或重演。	☐	☐	☐	☐	☐	
A.14.2	於開發及支援過程中之安全							
A.14.2.1 (建議)	保全開發政策	應建立軟體及系統開發之規則，並應用至施行單位內之開發。	☐	☐	☐	☐	☐	
A.14.2.2	系統變更控制程序	應藉由使用正式之變更控制程序，以控制開發生命周期內之系統變更。	☐	☐	☐	☐	☐	
A.14.2.3	運作平台變更後，應用之技術審查	當運作平台變更時，應審查及測試營運之關鍵應用，以確保對組織運作或安全無不利衝擊。	☐	☐	☐	☐	☐	

控制項	條文		稽核評分					稽核發現說明
			A	B	C	D	E	
A.14.2.4	軟體套件變更之限制	應不鼓勵修改軟體套件， 且僅限於必要變更，並應嚴格控制所有變更。	☐	☐	☐	☐	☐	
A.14.2.5	保全系統工程原則	保全系統之工程原則，應予建立、文件化、維持及應用於所有資訊系統實作工作。	☐	☐	☐	☐	☐	
A.14.2.6 (建議)	保全開發環境	對涵蓋整個系統開發生命周期之系統開發及整合工作，施行單位應建立並適切地保護安全開發環境。	☐	☐	☐	☐	☐	
A.14.2.7	委外開發	組織應監督及監視委外系統開發活動。	☐	☐	☐	☐	☐	
A.14.2.8 (I/P) (建議)	系統安全測試	於開發中，應實施安全功能之測試。	☐	☐	☐	☐	☐	
A.14.2.9 (I/P)	系統驗收測試	應建立新資訊系統、系統升級及新版本之驗收測試計畫及準則。	☐	☐	☐	☐	☐	
A.14.3	測試資料							
A.14.3.1	測試資料之保護	應小心選擇、保護及控制測試資料。	☐	☐	☐	☐	☐	
A.15	供應者關係							
A.15.1	供應者關係中之資訊安全							

控制項	條文		稽核評分					稽核發現說明
			A	B	C	D	E	
A.15.1.1 (I/P)	供應者關係之資訊安全政策	應與供應者議定並文件化，降低與供應者存取施行單位資產關聯之風險的資訊安全要求事項。	☐	☐	☐	☐	☐	
A.15.1.2 (I/P)	於供應者協議中闡明安全性	應與每個可能存取、處理、儲存或傳達資訊，或提供 IT 基礎建設組件資訊之供應者，建立及議定所有相關資訊安全要求事項。	☐	☐	☐	☐	☐	
A.15.1.3 (I/P) (建議)	資訊及通訊技術供應鏈	與供應者之協議，應包含因應與資訊及通訊技術服務及產品供應鏈關聯之資訊安全風險。	☐	☐	☐	☐	☐	
A.15.2	供應者服務交付管理							
A.15.2.1 (I/P)	供應者服務之監視及審查	組織應定期監視、審查及稽核供應者服務交付。	☐	☐	☐	☐	☐	
A.15.2.2 (I/P)	管理供應者服務之變更	應管理供應者所提供服務之變更，包括維持及改善既有的資訊安全政策、程序及控制措施，並考量所涉及之營運資訊、系統及過程的關鍵性，以及風險之重新評鑑。	☐	☐	☐	☐	☐	
A.16	資訊安全事故管理							
A.16.1	資訊安全事故及改善之管理							

控制項	條文		稽核評分					稽核發現說明
			A	B	C	D	E	
A.16.1.1 (I/P)	責任及程序	應建立管理責任及程序， 以確保對資訊安全事故做迅速、有效及有序之回應。	☐	☐	☐	☐	☐	
A.16.1.2 (I/P)	通報資訊安全事件	應循適切之管理管道，儘速通報資訊安全事件。	☐	☐	☐	☐	☐	
A.16.1.3 (I/P)	通報資訊安全弱點	應要求使用資訊系統及服務之員工及承包者，注意並通報任何系統或服務中所觀察到或可疑之資訊安全弱點。	☐	☐	☐	☐	☐	
A.16.1.4 (I/P)	資訊安全事件評估及決策	應評鑑資訊安全事件，並決定是否將其歸類為資訊安全事故。	☐	☐	☐	☐	☐	
A.16.1.5 (I/P)	對資訊安全事故之回應	應依文件化程序，回應資訊安全事故。	☐	☐	☐	☐	☐	
A.16.1.6 (I/P)	由資訊安全事故中學習	應使用獲自分析及解決資訊安全事故之知識，以降低未來事故之可能性及衝擊。	☐	☐	☐	☐	☐	
A.16.1.7 (I/P)	證據之收集	組織應定義及應用程序，以識別、蒐集、取得及保存可用作證據之資訊。	☐	☐	☐	☐	☐	
A.17	營運持續管理之資訊安全層面							
A.17.1	資訊安全持續							

控制項	條文		稽核評分					稽核發現說明
			A	B	C	D	E	
A.17.1.1	規劃資訊安全持續	施行單位應決定對其資訊安全之要求事項，以及在不利情況下（例：危機或災難期間），對資訊安全之持續性要求事項。	☐	☐	☐	☐	☐	
A.17.1.2	實作資訊安全持續	施行單位應建立、文件化、實作及維持過程、程序及控制措施，以確保在不利情況期間所要求之資訊安全持續等級。	☐	☐	☐	☐	☐	
A.17.1.3	查證、審查及評估資訊安全持續	組織應定期查證所建立及實作之資訊安全持續控制措施，以確保其於不良情況期間係生效及有效。	☐	☐	☐	☐	☐	
A.17.2	多重備援							
A.17.2.1	資訊設備之可用性	應對資訊處理設施實作充分之多重備援，以符合可用性要求。	☐	☐	☐	☐	☐	
A.18	遵循性							
A.18.1	對法律及契約要求事項之遵循							
A.18.1.1 (I/P)	適用之法規及契約的要求事項之識別	對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。	☐	☐	☐	☐	☐	
A.18.1.2	智慧財產權	應實作適切程序， 以確保遵循智慧財產權及專屬軟體產品使用之相關法律、法令及契約的要求事項。	☐	☐	☐	☐	☐	

控制項	條文		稽核評分					稽核發現說明
			A	B	C	D	E	
A.18.1.3 (I/P)	紀錄之保護	應依法令、法規、契約及營運要求保護紀錄，免於遺失、毀損、偽造、未授權存取及未經授權發布。	☐	☐	☐	☐	☐	
A.18.1.4 (I/P)	個人可識別資訊之隱私及保護	應依適用之相關法令、法規中之要求，以確保符合個人可識別資訊之隱私及保護。	☐	☐	☐	☐	☐	
A.18.1.5 (建議)	密碼式控制措施(加密控制措施)的監管	應使用密碼式控制措施(加密控制措施)，以遵循所有相關的協議、法律及法規。	☐	☐	☐	☐	☐	
A.18.2	資訊安全審查							
A.18.2.1 (I/P)	資訊安全之獨立審查	應依規劃之期間或當發生重大變更時， 獨立審查組織對管理資訊安全之作法及其實作（亦即資訊安全之各項控制目標、控制措施、政策、過程及程序）。	☐	☐	☐	☐	☐	
A.18.2.2 (I/P)	安全政策及標準之遵循性	管理人員應以適切之資訊安全政策、標準及其他安全要求事項，定期審查其責任範圍內之安全處理及程序的遵循性。	☐	☐	☐	☐	☐	
A.18.2.3 (I/P)	技術遵循性審查	應定期審查資訊系統對組織之資訊安全政策及標準的遵循性。	☐	☐	☐	☐	☐	

稽核人員：_____ 稽核日期：__