管理系統文件

文件類別	第二階文件	
文件編號	ISMS-P-007	
文件名稱	資通安全稽核管理程序書	
發行單位	文件管制小組	
發行日期	108 年 04 月 15 日	
版次	2.2	
訂修廢單位	審查	核准
資通安全處理小組		

（原版簽名頁保存於文件管制小組）

訂　　修　　廢　　記　　錄		
版次	發行日期	訂 修 廢 內 容 摘 要
2.0	104/04/30	2015 改版發行。
2.1	107/03/09	修改本文件內部稽核計畫單、內部稽核檢查單保存地點資訊科技中心單位名稱為圖書資訊處。
2.2	108/04/15	因應資通安全管理法修訂本文件

1. 目的

為查驗本校資訊安全管理制度（以下簡稱 ISMS）各項作業的控制目標、控制措施、流程及程序是否符合法規、ISO 標準及組織之資通安全要求，以確保各項業務能有效運作，特制訂本程序書。

2. 適用範圍

凡本校有關作業之內部稽核管理，均適用本程序書。

3. 參考文件

無。

4. 名詞定義

4.1. 內部稽核

對於資訊安全管理制度運作情形予以查驗，以判定系統之各項活動與其相關結果，是否符合預定計畫，及計劃事項是否有效執行，並能適切達到資通安全目標。內部稽核區分為定期稽核與不定期稽核兩類。

4.2. 定期稽核

依據定期頒布之稽核計畫內容，對各相關單位進行之內部稽核。

4.3. 不定期稽核

於必要時，對特定單位資通安全管理制度之運作，所執行之內部稽核。

4.4. 內部稽核人員

4.4.1. 由管理代表遴選適當合格之內部稽核人員，依需要進行任務編組以執行內部稽核。

4.4.2. 受過內部稽核人員訓練課程者，含校內及派外訓練得有證書者，始得任用為內部稽核人員。

5. 作業內容

5.1. 資通安全稽核管理流程圖

作業流程	權責單位	相關表單
稽核計畫擬定	執行秘書	內部稽核計畫單
No / 審核	資通安全長	內部稽核計畫單
Yes / 發出稽核通知	內部稽核小組	內部稽核檢查單
召開啟始會議	執行秘書	會議紀錄單
執行稽核	內部稽核小組	內部稽核檢查單
撰寫稽核報告	內部稽核小組	矯正及預防處理單
召開總結會議	執行秘書	會議紀錄單
執行矯正措施	受稽單位	矯正及預防處理單
No / 效果確認	內部稽核小組	
Yes / 稽核結果彙整	執行秘書	矯正及預防處理單
提報管理審查	執行秘書	矯正及預防處理單
紀錄保存	資通安全處理小組	

5.2. 稽核人員組成

5.2.1. 由執行秘書遴選適當合格之內部稽核人員，組成資安稽核小組，以執行內部稽核作業。

5.2.2. 受過內部稽核人員訓練課程者，始得任用為內部稽核人員。

5.3. 稽核計畫擬訂

5.3.1. 定期性

5.3.1.1. 資通安全內部稽核作業，應每一年執行一次。

5.3.1.2. 排定稽核計畫時，需注意稽核人員與被稽核之單位及作業不應有直接關係，以確保稽核過程的客觀性與獨立性。

5.3.1.3. 由執行秘書或其指定之人員於每次執行前，擬妥「ISMS-P-007-01 內部稽核計畫單」後，經資通安全長核准後實施。

5.3.1.4. 若稽核計畫有異動時，應由資通安全長審核後實施。

5.3.2. 非定期性

執行秘書於下列時機，得隨時召集資安稽核小組，到特定單位或範圍執行非例行性之稽核作業：

5.3.2.1. 各單位業務重大變動時。

5.3.2.2. 內部稽核完畢後之跟催。

5.3.2.3. 其它需非定期性稽核時機。

5.4. 發出稽核通知

5.4.1. 執行秘書於稽核前應召集資安稽核小組成員，召開小組準備會議，分派任務、協調分工、說明稽核重點以及訂定稽核時間。

5.4.2. 資安稽核小組所有成員應針對本次負責之部分，先了解各相關規定程序及標準，並詳讀上次稽核之缺點報告，以研擬此次稽核之重點，並編寫於「ISMS-P-007-02 內部稽核檢查單」上，呈核後影印一份給受稽核單位主管，做為對受稽單位稽核通知使用。

5.4.3. 受稽單位於接獲稽核通知後，應配合準備稽核所需之相關資料。

5.5. 召開啟始會議

執行秘書可視需要於稽核開始前，召集資安稽核小組及受稽單位召開「啟始會議」，說明稽核方式、範圍、時程、配合事項以及進行其他事前溝通。此啟始會議由執行秘書指派特定人員負責紀錄，並填寫於「ISMS-P-002-03 會議紀錄單」。

5.6. 執行稽核

5.6.1. 稽核人員依「ISMS-P-007-02 內部稽核檢查單」上之查檢項目，先實地檢查作業狀況及書面資料，再與經辦人員面談實際作業狀況。

5.6.2. 稽核時，稽核人員應秉持公正、謹慎客觀、友善之態度進行查核工作，並且以協助者態度發現缺點，不任意批評而以客觀建議方式要求修正。

5.6.3. 稽核人員於稽核時，應依抽樣之原理收集足夠之客觀證據，研判該稽核項目是否符合相關規範，稽核時應保存適當的稽核軌跡，其稽合結果可分符合、不符合、不適用三種。

5.6.3.1. 符合：以「○」符號表示，表實際作業確實符合稽核要項之規範、要求。

5.6.3.2. 不符合：以「╳」符號表示，表實際作業完全或部份未達稽核要項之規範、要求。

5.6.3.3. 不適用：以「＼」符號表示，表實際作業未發生稽核要項之規範、要求或時間點未到，以致稽核時無法確認、判斷。

5.6.4. 受稽單位應尊重及支持稽核人員，誠實答覆稽核人員所提問題，並接受調閱相關的紀錄、報告及文件資料。

5.7. 撰寫稽核報告

5.7.1. 內部稽核人員於稽核後應盡可能收集客觀證據，將發現之缺失及與受稽單位研討之改善措施撰寫於「ISMS-P-008-01 矯正及預防處理單」，請受稽單位提出改善期限並簽名確認後呈核。

5.7.2. 記錄時，應盡可能將相關之人、事、時、地、物以及違反之規定或條款填寫清楚，以利日後之追溯。

5.8. 召開總結會議

5.8.1. 稽核人員應將稽核結果透過資安稽核小組內部會議討論、彙整後由執行秘書提出稽核報告。

5.8.2. 執行秘書應於稽核完成後，召開「總結會議」，說明稽核結果及發現，並對各項疑義進行澄清。此總結會議由執行秘書指派特定人員負責紀錄，並填寫於「ISMS-P-002-03 會議紀錄單」。

5.9. 執行矯正措施

5.9.1. 各受稽單位應於改善期限前完成矯正措施，以維持資訊安全管理制度正常運作。

5.9.2. 各內部稽核人員應於改善期限後追蹤確認缺點之改善情形，於「ISMS-P-008-01 矯正及預防處理單」中敘述追蹤狀況，並呈執行秘書、資通安全長。

5.9.3. 若追蹤結果仍有問題，亦應將其狀況再度紀錄於「ISMS-P-008-01 矯正及預防處理單」呈核加以追蹤，直至改善完成為止。

5.10. 提報管理審查

稽核人員於稽核完成後，應將「ISMS-P-008-01 矯正及預防處理單」交執行秘書彙總，以提報管理審查會議。

5.11. 相關法令之要求

本校執行業務時，應遵守相關法令、法規之要求，資安稽核小組亦應於每次進行資安稽核時檢視其符合性。

5.12. 紀錄保存

相關業務承辦人員應參照如下規範，妥善保存各項紀錄。

編號	表單名稱	保存地點	保存期限
1	內部稽核計畫單	圖書資訊處	至少 1 年
2	內部稽核檢查單	圖書資訊處	至少 1 年

6. 附件

6.1. ISMS-P-007-01 內部稽核計畫單。

6.2. ISMS-P-007-02 內部稽核檢查單。

6.3. ISMS-P-002-03 會議紀錄單。

6.4. ISMS-P-008-01 矯正及預防處理單。

開　南　大　學
K A I N A N　U n i v e r s i t y

內　部　稽　核　計　畫　單

年　　度		稽核類別	□定期稽核　□不定期稽核
稽核日期	受稽單位	稽核人員	內部稽核要項

稽核組長		主管審核	

開南大學
KAINAN University

內部稽核檢查單

稽核項目		受稽單位		稽核人員		稽核日期	

章節	稽核要點	稽核結果			稽核發現
		符合	不符合	不適用	
4.	**組織背景**				
4.1	**了解組織與其背景** 組織應決定與其目的相關，且會影響其 ISMS 預期結果的達成能力之外部與內部問題。				
4.2	**了解利害相關團體的需求與期望** 組織應決定： a) 與 ISMS 有關的利害相關團體；以及 b) 與資訊安全有關的這些利害相關團體之要求。				
4.3	**決定資訊安全管理系統的適用範圍** 組織應決定ISMS的界線與適用性，以建立其適用範圍。當決定適用範圍時，組織應考量： a) 4.1 所提到的外部與內部問題； b) 4.2 所提到的要求；以及 c) 在組織與其他組織執行的活動之間的接合與互賴關係。				
4.4	**資訊安全管理系統** 組織應依據本標準的要求，以建立、實施、維持和持續改進ISMS。				
5.	**領導力**				
5.1	**領導力與承諾** 高階管理者應展現領導力，以及與 ISMS 有關的承諾，藉由： a) 確保資訊安全政策與目標已建立，並且和組織的策略方向是相容的； b) 確保 ISMS 的要求已融入組織過程中； c) 確保 ISMS 所需的資源可取得； d) 傳達有效資訊安全管理的重要性，並且遵守 ISMS 的要求； e) 確保 ISMS 達成其預期效果； f) 指導與支援人員，使其對 ISMS 的有效性做出貢獻； g) 促進持續改進；以及				

開 南 大 學
K A I N A N U n i v e r s i t y

章節	稽核要點	稽核結果			稽核發現
		符合	不符合	不適用	
	h) 支援其他的相關管理角色，讓其展現出在職責運用上之領導力。				
5.2	**政策** 高階管理者應建立一個資訊安全政策，是： a) 符合組織目的； b) 包含資訊安全目標(見 6.2)，或提供訂立資訊安全目標的框架； c) 包含對滿足有關資訊安全之適用要求的承諾；以及 d) 包含對 ISMS 持續改進的承諾。 資訊安全政策應為文件化資訊並可取得： －在組織內流通；以及 －適當時，利害相關團體可取得。				
5.3	**組織角色、責任與職權** 高階管理者應確保有關資訊安全的角色之責任與職權已分配和傳達。 高階管理者應分配責任與職權，以： a) 確保 ISMS 遵守本標準的要求；以及 a) 報告 ISMS 的績效給高階管理者。				
6.	**計畫**				
6.1	**風險與機會的應對措施**				
6.1.1	**概述** 當計劃ISMS時，組織應考量4.1所提到的問題與4.2所提到的要求，並且決定需要應對的風險與機會。				
6.1.2	**資訊安全風險評鑑** 組織應明訂一個資訊安全風險評鑑的過程，可： a) 建立與維持資訊安全風險的標準 b) 確保重複的資訊安全風險評鑑能產出一致的、有效的和可比較的結果； c) 識別資訊安全風險 d) 分析資訊安全風險 e) 評估資訊安全風險 組織應保存有關資訊安全風險評鑑過程的文件化資訊。				
6.1.3	**資訊安全風險處理** 組織應明訂與適用一個資訊安全處理過程，以：				

開南大學
KAINAN University

章節	稽核要點	稽核結果			稽核發現
		符合	不符合	不適用	
	a) 選擇適當的資訊安全風險處理之選項，將風險評鑑結果列入考量； b) 決定在實施選用的資訊安全處理選項時，必需的所有管制項； a) 備考：組織可依據需要設計管制，或從任何來源識別它們。 b) 比較在上述6.1.3b)決定的管制與附錄A的，且確認沒有忽略到必要的管制； c) 創作一個適用性的聲明，要包含必需的管制(見6.1.3b)與c)，以及無論是否進行實施，包含之正當理由，還有附錄A的管制排除之正當理由； d) 制定一個資訊安全風險處理計畫； e) 獲得風險負責人對資訊安全風險處理計畫的核准，以及接受殘留的資訊安全風險。 組織應保存資訊安全風險處理過程的文件化資訊。				
6.2	**資訊安全目標與實現的計畫** 組織應在相關的職能與層級上，建立資訊安全目標。 資訊安全目標應： a) 與資訊安全政策一致； b) 可測量(如果可行時)； c) 考量適用的資訊安全要求，以及風險評鑑與處理結果； d) 經過溝通，且 e) 適當時作更新。 組織應保存資訊安全目標的文件化資訊。 當計劃如何達成其資訊安全目標時，組織應決定： f) 要做什麼； g) 需要什麼資源； h) 誰要負責； i) 何時完成；且 j) 如何評估結果。				
7.	**支援**				
7.1	**資源** 組織應決定與提供用來建立、實施、維持和持續改進 ISMS 所需的資源。				
7.2	**人員能力** 組織應：				

開 南 大 學
K A I N A N U n i v e r s i t y

章節	稽核要點	稽核結果			稽核發現
		符合	不符合	不適用	
	a) 決定會影響資訊安全績效，受其管制的工作人員所必需的能力； b) 確保這些人員能勝任，以適當的教育、訓練或經驗為根據； c) 適用時，採取措施以取得必需的能力，且評估採取的措施之有效性；以及 d) 保存適當的文件化資訊當作能力的證據。				
7.3	**認知** 受組織管制的工作人員應認知到： a) 資訊安全政策； b) 對ISMS有效性之貢獻，包含了改進資訊安全績效之好處；以及 c) 不符合ISMS要求的含義。				
7.4	**溝通** 組織應決定與ISMS有關的內部與外部溝通之需求，包含了： a) 要溝通什麼； b) 何時溝通； c) 和誰溝通； d) 應是誰溝通；以及 e) 應實現哪種溝通過程。				
7.5	文件化資訊				
7.5.1	**概述** 組織的ISMS應包含： a) 本標準必需的文件化資訊；以及 b) 由組織決定，ISMS的有效性所必需的文件化資訊。				
7.5.2	**創造與更新** 當創造與更新文件化資訊時，組織應確保適當的： a) 識別與描述(例如一個標題、日期、作者、或參考編號)； b) 格式(例如語言、軟體版本、圖表)與媒介(例如紙本、電子)；以及 c) 適用性與充足性的審查和核准。				
7.5.3	**文件化資訊的管制** ISMS與本標準必需的文件化資訊應受管制以確保： a) 在需要的地點與時間，可取得且適當使用； b) 受到充分的維護(例如避免機密性的損害、使用不當、或完整性的損害)；				

開 南 大 學
K A I N A N U n i v e r s i t y

章節	稽核要點	稽核結果			稽核發現
		符合	不符合	不適用	
	對於文件化資訊的管制，適用時，組織應應對下列的活動： c) 分配、存取、修復、使用； d) 貯藏與保存，包含保存易讀性； e) 變更管制(例如版本的變更)；以及 f) 保留與廢除。 由組織決定，ISMS的計畫與運作所必需的外部來源之文件化資訊，適當時應識別之且接受管制。				
8.	**運作**				
8.1	**運作的計畫與管制** 組織應計畫、實施與管制可符合資訊安全要求，及實施在6.1決定的措施時所需要的過程。組織也應實施計畫，以達成在6.2決定的資訊安全目標。 組織應依照計畫實現過程所必需的信心程度，保存文件化資訊。 組織應管制計畫的變更，並審查無預期的變更會帶來的後果，在必要時，採取措施以減輕任何不良影響。 組織應確保外包過程是確定的並受管制。				
8.2	**資訊安全風險評鑑** 組織應在計劃之期間內，或是當重大的變更被提出或發生時，執行資訊安全風險評鑑，並考量在6.1.2a)建立的標準。 組織應保存資訊安全風險評鑑結果的文件化資訊。				
8.3	**資訊安全風險處理** 組織應實施資訊安全風險處理的計畫。 組織應保存資訊安全風險處理結果的文件化資訊。				
9.	**績效評估**				
9.1	**監督、量測、分析與評估** 組織應評估資訊安全的績效與ISMS的有效性。 a) 什麼需要監督與量測，包含資訊安全過程與管制； b) 監督、量測、分析與評估的方法，適用時，用以確保有效的結果； c) 監督與量測應何時執行； d) 應由誰監督與量測； e) 從監督與量測得來的結果應何時分析與評估；以及				

章節	稽核要點	稽核結果			稽核發現
		符合	不符合	不適用	
	f) 應由誰分析與評估這些結果。 組織應保存適當的文件化資訊，作為監督與量測結果的證據。				
9.2	**內部稽核** 組織應在計劃之期間內執行內部稽核，以提供資訊，指出ISMS是否： a) 符合 – 組織本身有關ISMS的要求；以及 – 本標準的要求； b) 有效地實施與維護。 組織應： c) 計畫、建立、實施與維護一個稽核流程，包含了頻率、方法、責任、計畫中的要求與報告。稽核流程應考量相關過程的重要性，以及先前稽核的結果； d) 為每一場稽核明訂稽核標準與適用範圍； e) 選擇稽核員並執行稽核，以確保稽核過程的客觀與公正； f) 確保稽核結果已向相關管理者報告；以及 g) 保存文件化資訊，作為稽核流程與稽核結果的證據。				
9.3	**管理階層審查** 高階管理者應在時間間隔內審查組織的ISMS，以確保其持續的適用性、充足性與有效性。 管理審查應包含的考量事項： a) 先前管理審查的措施之狀態 b) 有關ISMS的外部與內部問題之變更； c) 資訊安全的績效回饋，包含下列趨向： – 不符合事項與矯正措施； – 監督與量測結果； – 稽核結果；以及 – 資訊安全目標的實現； d) 利害相關團體的回饋； e) 風險評鑑的結果與風險處理計畫的狀態；以及 f) 持續改進的機會； 管理審查的產出應包含和持續改進機會與ISMS的變更需求有關之決定。 組織應保存文件化資訊，管理審查結果的證據。				

開 南 大 學
K A I N A N U n i v e r s i t y

章節	稽核要點	稽核結果			稽核發現
		符合	不符合	不適用	
10.	**改進**				
10.1	**不符合事項與矯正措施** 當一個不符合事項發生，組織應： a) 適用時，對不符合事項作出回應： －採取措施管制與矯正之；以及 －處理後果； b) 評估消除不符合事項的原因之措施需求，為了使其不再發生或是在別處發生，經由： －審查不符合事項； －決定不符合事項的原因；以及 －決定是否有相似的不符合事項存在，或有發生的潛在性； c) 實施任何需要的措施； d) 審查任何採取的矯正措施之有效性；以及 e) 必要時，對ISMS作變更； 矯正措施應適用於所遇到的不符合事項之影響。 組織應保存文件化資訊，作為下列證據： f) 不符合事項的本質與任何採取的後續措施；以及 g) 任何矯正措施的結果。				
10.2	**持續改進** 組織應持續改進ISMS的適切性、充分性與有效性。				
A.5	**資訊安全政策**				
A.5.1	**資訊安全的管理方向** 是否有建立書面程序以檢視組織是否依照營運要求及相關法律規章，提供管理階層對資訊安全的指示與支持（資訊安全政策是否適當、合法）。				
A.5.1.1	**資訊安全政策** 資訊安全相關政策是否由管理階層定義及核准，並公布傳達給所有員工與相關外部團體。				
A.5.1.2	**資訊安全政策之審查** 資訊安全政策是否有定期或有重大變更時審查，以確保持續的適當性、充分性、及有效性。				

開南大學
KAINAN University

章節	稽核要點	稽核結果			稽核發現
		符合	不符合	不適用	
A.6	**資訊安全的組織**				
A.6.1	**內部組織** 組織內部資訊安全的管理是否有建立組織系統以檢視其運作。				
A.6.1.1	**資訊安全的角色與責任** 是否明確定義所有資訊安全的責任歸屬。				
A.6.1.2	**職務的區隔** 是否有區分具衝突之職務與責任範圍，以降低組織資產遭未經授權或非意圖的修改或誤用之機會。				
A.6.1.3	**與權責機關的聯繫** 是否有建立書面程序與有關當局維持適當聯繫。				
A.6.1.4	**與特殊利害相關團體的聯繫** 是否與各特殊利害相關團體或其他各種專家安全論壇及專業協會維持適當聯繫。				
A.6.1.5	**專案管理的資訊安全** 不論專案之類型、大小、時程長短及範圍為何，資訊安全要求是否在專案管理中被明確陳述與實作。				
A.6.2	**行動設備與遠距工作** 是否有建立對應方法或程序以確保遠距工作與使用行動式電腦裝置之資訊安全。				
A.6.2.1	**行動設備的政策** 是否有制定正式政策及採取適當的安全措施，以管理及因應因使用行動式電腦與通訊設施所導致的風險。				
A.6.2.2	**遠距工作** 是否有制定正式政策及採取適當的安全措施，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	**聘僱之前** 是否有建立書面程序以確保受僱人員、承包商及第三方使用者了解其職責，並適合其所被認定及考慮的角色，以降低設施的盜竊、詐欺或誤用風險。				
A.7.1.1	**篩選** 是否依照相關法律、規章與倫理，並兼顧營運要求的適切性、所存取資訊的保密分類以及所認知的風險，對所受僱的人員、承包商及第三方使用者進行背景查證與核對。				

開南大學
KAINAN University

章節	稽核要點	稽核結果			稽核發現
		符合	不符合	不適用	
A.7.1.2	**聘僱條款與條件** 與受僱人員、承包商及第三方使用者簽訂契約時，是否有將保密條款與資訊安全責任納入契約條款中，視為契約責任的一部份。				
A.7.2	**聘僱期間** 是否有建立書面程序以確保受僱人員、承包商及第三方使用者了解資訊安全的威脅與問題、本身的責任與義務、且有能力在日常工作中支持組織安全政策，降低人為錯誤的風險。				
A.7.2.1	**管理階層責任** 管理當局是否有要求受僱人員、承包商及第三方使用者依照組織已制定的政策及程序是否有用安全。				
A.7.2.2	**資訊安全認知、教育及訓練** 組織所有受僱人員及相關的承包商及第三方使用者是否有接受與其工作功能相關，適當的認知訓練與組織政策及程序的定期更新。				
A.7.2.3	**懲處過程** 對違反安全的受僱人員，是否有建立正式的懲罰過程並執行。				
A.7.3	**聘僱的終止與變更** 是否有建立書面程序以確保員工及承包商以有條理的方式變更或終止聘僱，以保護組織之利益。				
A.7.3.1	**聘僱責任的終止與變更** 在聘僱終止或變更後持續有效的資訊安全責任與義務是否已明確定義與執行，並適時向員工及承包者溝通及宣導。				
A.8	**資產管理**				
A.8.1	**資產責任** 是否有建立書面程序識別組織資產及定義適切的保護責任。				
A.8.1.1	**資產清冊** 是否已明確識別與資訊及資訊處理設施有關的資產，並製作與維護上述資產的清冊。				
A.8.1.2	**資產的擁有權** 資產清冊中被維護的資產是否已明確指派擁有者，進行資產管理。				
A.8.1.3	**資產之可被接受的使用** 與資訊處理設施相關的資訊及資產，其可接受使用的規則是否已經予以有效識別、記				

開 南 大 學
K A I N A N U n i v e r s i t y

章節	稽核要點	稽核結果			稽核發現
		符合	不符合	不適用	
	錄及實作。				
A.8.1.4	**資產歸還** 所有員工及承包商在終止其聘僱、合約或協議時是否有歸還其擁有的所有組織的資產。				
A.8.2	資訊分類 是否確認所有資產能依據對組織之重要性，獲得適切程度的保護。				
A.8.2.1	**資訊分類** 資訊是否依其對組織的法律要求、價值、重要性及對未經授權揭露或修改之敏感性加以分類。				
A.8.2.2	**資訊標示** 是否依照組織所採用的資訊分類法，發展與實作一套適當的資訊標示程序。				
A.8.2.3	**資產處置** 是否依照組織所採用的資訊分類法，發展與實作處置資產之程序。				
A.8.3	**媒體的處置** 是否有建立書面程序以防止儲存於媒體之資訊被未經授權的揭露、修改、移除或破壞。				
A.8.3.1	**可攜式媒體的管理** 是否已依照組織所採用的資訊分類法，實施適當的可攜式媒體之管理程序。				
A.8.3.2	**媒體的處理** 媒體不再使用時，是否有使用正式程序安全穩固地報廢。				
A.8.3.3	**實體媒體的傳送** 是否有保護含有資訊的媒體在傳送時，使其不受未經授權的存取、誤用或毀損的風險。				
A.9	存取控制				
A.9.1	**存取控制的營運要求** 是否有建立書面程序以控制資訊及資訊處理設施的存取。				
A.9.1.1	**存取控制政策** 是否有建立、文件化、及依據存取的營運與安全要求審查存取控制政策。				
A.9.1.2	**網路與網路服務的存取** 是否僅提供使用者經特定授權可存取使用的網路與網路服務。				
A.9.2	**使用者存取管理** 是否有建立書面程序以確保經授權使用者對系統與服務的存取與防止未經授權的存				

開 南 大 學
K A I N A N U n i v e r s i t y

章節	稽核要點	稽核結果			稽核發現
		符合	不符合	不適用	
	取。				
A.9.2.1	**使用者登錄與註銷** 是否建立及實施正式的使用者登錄與註銷登錄程序，以便能指派存取權限。				
A.9.2.2	**使用者的存取配置** 是否已建立及實施正式的使用者配置程序，以對所有資訊系統與服務指派和撤銷存取。				
A.9.2.3	**特權的管理** 是否有限制與控制特權的分配與使用。				
A.9.2.4	**使用者的機密授權資訊之管理** 是否有以正式的管理過程控制機密鑑別資訊的分配。				
A.9.2.5	**使用者存取權限的審查** 資產擁有者是否定期審查使用者的存取權限。				
A.9.2.6	**存取權限的移除或調整** 所有員工及外部團體使用者對資訊及資訊處理設施的存取權限，是否在其聘僱、合約或協議終止時，或因變更而調整時予以移除。				
A.9.3	**使用者責任** 是否讓使用者為其鑑別資訊之安全防護負責。				
A.9.3.1	**機密授權資訊的使用** 是否有要求使用者遵照組織的良好安全方式，使用機密鑑別資訊。				
A.9.4	**系統與應用系統的存取控制** 是否建立書面程序及對應方法以防止作業系統與應用系統遭未經授權的存取。				
A.9.4.1	**資訊存取限制** 是否有根據已定義的存取控制政策，限制對資訊與應用系統功能之存取。				
A.9.4.2	**安全之登入程序** 在存取控制政策要求之下，是否已由安全登入程序控制對系統與應用系統之存取。				
A.9.4.3	**通行碼管理系統** 通行碼管理系統是否為互動式，且確保通行碼嚴謹。				
A.9.4.4	**特權的公用程式之使用** 是否有限制與嚴密控制可能能夠置換系統與應用控制措施的公用程式之使用。				
A.9.4.5	**程式原碼的存取控制**				

開 南 大 學
K A I N A N U n i v e r s i t y

章節	稽核要點	稽核結果			稽核發現
		符合	不符合	不適用	
	是否有限制對程式原始碼的存取。				
A.10	**密碼**				
A.10.1	**密碼控制措施** 是否有建立對應方法或程序以藉由密碼方式保護資訊的機密性、鑑別性或完整性。				
A.10.1.1	**使用密碼控制措施的政策** 是否有發展與實作使用密碼控制措施以保護資訊的政策。				
A.10.1.2	**金鑰管理** 是否在密碼金鑰之整個生命週期發展與實作密碼金鑰之使用、保護與生命期的政策。				
A.11	**實體與環境安全**				
A.11.1	**安全區域** 是否有建立書面程序以防止組織資訊與資訊處理設施遭未經授權的實體存取、損害及干擾。				
A.11.1.1	**實體安全邊界** 是否使用用安全邊界（例如牆、磁卡控制的大門或人工駐守的櫃檯等屏障），以保護含有敏感或重要資訊及資訊處理設施的區域。				
A.11.1.2	**實體進出管制** 安全區域是否有適當的進入控制措施，以確保只有授權人員方可進出。				
A.11.1.3	**實施辦公場所及設施之安全管制** 是否有設計與是否有用辦公室及設施的實體安全。				
A.11.1.4	**對外部與環境威脅的保護** 是否設計與是否有用實體保護，不受火災、洪水、地震、爆炸、民間暴動、及其它自然或人為災難的損害。				
A.11.1.5	**在安全區域內工作** 是否有設計與應用在保全區域內工作的程序。				
A.11.1.6	**收發與裝卸區** 是否有控制收發裝卸區及其它未經授權人員可進入邊界點等存取點，若可能，隔離資訊處理設施以防止未經授權的存取。				
A.11.2	**設備** 是否有建立書面程序防止資產遺失、損害、偷竊或受損，並防止組織活動中斷。				

開 南 大 學
K A I N A N U n i v e r s i t y

章節	稽核要點	稽核結果			稽核發現
		符合	不符合	不適用	
A.11.2.1	**設備安置與保護** 是否安置或保護設備，以降低來自環境之威脅與危機造成的風險，以及未經授權存取之機會。				
A.11.2.2	**支援的設施** 應保護設備不受電源失效及其他支援的公用設施失效所導致的中斷				
A.11.2.3	**佈纜的安全** 是否有保護傳送資料或支援資訊服務之電源與電信纜線，以防止竊聽或損害。				
A.11.2.4	**設備維護** 是否有正確地維護設備，確保其持續的可用性與完整性。				
A.11.2.5	**資產的攜出** 是否有未經事前授權，設備、資訊或軟體帶至場外。				
A.11.2.6	**駐外設備的安全** 適用於場外設備的安全，是否有考慮在組織邊界外工作的不同風險。				
A.11.2.7	**設備的汰除或再使用之安全** 在報廢前是否有核對所有包含儲存媒體的設備，確保任何敏感性資料及授權的軟體已被移除或安全地覆寫。				
A.11.2.8	**無人看管的用戶設備** 使用者是否有確保無人看管的資訊設備有適當保護措施。				
A.11.2.9	**桌面淨空與螢幕淨空政策** 是否有採取文件與可攜式儲存媒體的桌面淨空政策及資訊處理設施的螢幕淨空政策。				
A.12	**作業的安全**				
A.12.1	**作業之程序與責任** 是否有建立書面程序以確保正確與安全地操作資訊處理設施。				
A.12.1.1	**文件化作業程序** 作業程序是否加以文件化並讓有需要的所有使用者均可隨時取得。				
A.12.1.2	**變更管理** 會影響資訊安全的組織、營運過程、資訊處理設施與系統的變更是否已受到控制。				
A.12.1.3	**容量管理** 資源的使用是否有監控、調校、及預估未來容量需求，以確保所需的系統執行績效。				

開南大學
KAINAN University

章節	稽核要點	稽核結果			稽核發現
		符合	不符合	不適用	
A.12.1.4	**開發、測試及運作環境的分隔** 是否有分隔開發、測試及運作環境，以降低對作業系統未經授權存取或變更的風險。				
A.12.2	**防範惡意程式** 是否有建立書面程序以確保資訊與資訊處理設施可防範惡意軟體。				
A.12.2.1	**對抗惡意程式的控制措施** 是否有實作防範惡意碼的偵測、預防、及復原控制措施與適當之使用者認知程序。				
A.12.3	**備份** 是否有建立程序以防範資料之損失(完整性喪失)。				
A.12.3.1	**資訊備份** 是否有依據所議定的備份政策，定期進行資訊、軟體與系統影像的備份與測試。				
A.12.4	**存錄與監控** 是否有建立書面程序以紀錄事件及產生證據。				
A.12.4.1	**事件存錄** 是否有產生、保留與定期審查記錄使用者活動、異常、失誤及資訊安全事件之事件日誌。				
A.12.4.2	**日誌資訊的保護** 是否有保護記錄日誌設施與日誌資訊，不受竄改及未經授權的存取。				
A.12.4.3	**管理者與操作員日誌** 是否有記錄系統管理者與操作者的活動日誌，且保護與定期審查該日誌。				
A.12.4.4	**時脈同步** 組織或安全領域內所有相關資訊處理系統的時脈是否與公認的準確時間來源同步。				
A.12.5	**作業軟體的控制** 是否有建立對應方法或程序以確保作業系統之完整性。				
A.12.5.1	**作業系統上軟體的安裝** 是否有備妥各項適當程序以控制作業系統上軟體的安裝。				
A.12.6	**技術脆弱性管理** 是否有建立對應方法或程序以降低利用已公佈的技術脆弱性導致的風險。				
A.12.6.1	**技術脆弱性的管理** 是否有及時的取得關於使用中資訊系統之技術脆弱性的資訊、並評估組織對此等脆弱性的暴露，以及採取適當的措施以因應相關的風險。				

開南大學
KAINAN University

章節	稽核要點	稽核結果			稽核發現
		符合	不符合	不適用	
A.12.6.2	**軟體安裝的限制** 是否已建立與實施使用者安裝軟體的管控規則。				
A.12.7	**資訊系統稽核考量** 是否有建立對應方法或程序以使稽核活動對運作中系統之影響降至最低。				
A.12.7.1	**資訊系統稽核控制** 有關作業系統查核之稽核要求與活動是否有仔細規劃與協議，以使營運過程中斷之風險降至最低。				
A.13	**通訊安全**				
A.13.1	**網路安全管理** 是否有建立書面程序以管理與控制網路，以保護系統與應用程式內的資訊。				
A.13.1.1	**網路控制措施** 是否有充分地管理與控制網路，使不受威脅，並且維護使用網路的系統與是否有用，包括傳輸中的資訊之安全。				
A.13.1.2	**網路服務的安全** 是否有識別所有網路服務的安全機制、服務等級及管理要求，並納入不論是內部或外包的任何網路服務協議。				
A.13.1.3	**網路區隔** 是否有區隔在網路上的資訊服務、使用者及資訊系統群組。				
A.13.2	**資訊轉換** 是否有建立書面程序以維護組織內與任何外部個體的資訊與軟體傳送之安全。				
A.13.2.1	**資訊轉換政策與程序** 是否有適當的正式交換政策、程序及控制措施，以保護經由使用所有型式通訊設施的資訊傳送。				
A.13.2.2	**資訊轉換的協議** 組織與外部團體間營運資訊的安全傳送是否建立協議。				
A.13.2.3	**電子傳訊** 是否有適當地保護涉及電子傳訊的資訊。				
A.13.2.4	**機密性或不揭露協議** 是否有識別、定期審查與文件化反映組織對資訊保護之需求的機密性或保密協議要求事項。				

開 南 大 學
K A I N A N U n i v e r s i t y

章節	稽核要點	稽核結果			稽核發現
		符合	不符合	不適用	
A.14	**資訊系統獲取、開發及維護**				
A.14.1	**資訊系統的安全要求** 是否有建立對應方法或程序以確保安全是整體資訊系統的一部分。這也包含在提供有關公共網路服務之資訊系統的要求中。				
A.14.1.1	**資訊安全要求分析與規格** 新資訊系統或現有資訊系統提升的營運要求聲明中，是否詳述安全控制措施的要求。				
A.14.1.2	**公共網路應用系統之安全服務** 是否保護在公用網路上傳輸而涉及電子商務的資訊，使不受詐欺行為、合約爭議及未經授權的揭露與修改。				
A.14.1.3	**保護應用系統服務之交易** 是否保護涉及線上交易的資訊，以防止不完整的傳輸、錯誤的路由、未經授權的訊息交替、未經授權的揭露及未經授權的訊息複製或重送。				
A.14.2	**開發與支援過程的安全** 是否確保資訊安全被整合至資訊系統開發生命週期之設計與實施之中。				
A.14.2.1	**安全開發政策** 是否建立軟體與系統的開發規則，並適用於組織內的開發。				
A.14.2.2	**系統變更控制程序** 變更的實作是否有使用正式變更控制程序予以控制。				
A.14.2.3	**作業平台變更後的應用系統技術審查** 當作業系統變更時，是否審查與測試關鍵應用系統，以確保對組織作業或安全無不利的衝擊。				
A.14.2.4	**套裝軟體變更的限制** 是否有適當管制以阻止修改套裝軟體，僅限有必要的變更，是否有嚴格管制所有的修改。				
A.14.2.5	**安全系統工程原則** 是否建立安全系統工程的原則並予維護及文件化，且適用於任何資訊系統的實施工作。				
A.14.2.6	**安全開發環境** 組織是否對涵蓋整個系統的開發與整合工作，建立安全開發環境並予適當地保護。				
A.14.2.7	**委外開發**				

開　南　大　學
K A I N A N　U n i v e r s i t y

章節	稽核要點	稽核結果			稽核發現
		符合	不符合	不適用	
	當軟體開發委外時，組織是否有妥當監督與監控。				
A.14.2.8	**系統安全測試** 安全功能的測試是否在開發期間進行。				
A.14.2.9	**系統驗收測試** 是否有建立對新資訊系統、系統升級及新版本的驗收準則，且開發期間與驗收前是否有完成適當之系統測試。				
A.14.3	**測試資料** 是否慎選、保護及管制測試資料。				
A.14.3.1	**測試資料的保護** 是否有小心地選擇測試資料，並保護及控制。				
A.15	**供應商關係**				
A.15.1	**供應商關係的資訊安全** 是否確保供應商可存取之組織資產的保護。				
A.15.1.1	**供應商關係的資訊安全政策** 是否與供應商協議資訊安全要求，以減少供應商對組織資產存取的風險並加以文件化。				
A.15.1.2	**供應商協議內的安全處理** 涉及存取、處理、通訊或管理組織的資訊或資訊處理設施，或在資訊處理設施上增加產品或服務的第三方合約，是否涵蓋所有相關的安全要求。				
A.15.1.3	**ICT供應鏈** 與供應商的協議，是否包含因應有關資訊與通訊技術服務及產品供應鏈之資訊安全風險的要求。				
A.15.2	**供應商服務交付管理** 是否有建立書面程序以實作與維護適當等級並與第三方服務遞送協議一致之資訊安全及服務遞送。				
A.15.2.1	**供應商服務的監控與審查** 是否有定期監控與審查由第三方提供的服務、報告及記錄，並定期實行稽核。				
A.15.2.2	**供應商服務變更的管理** 考慮牽涉到營運系統及過程的重要性與重新評鑑的風險，是否有管理服務條款的變更，包括維護及改善現存的資訊安全政策、程序及控制措施。				

開南大學
KAINAN University

章節	稽核要點	稽核結果			稽核發現
		符合	不符合	不適用	
A.16	**資訊安全事故管理**				
A.16.1	**資訊安全事故與改進的管理** 是否有建立對應方法或程序以確保實施一致與有效的方法管理資訊安全事故。				
A.16.1.1	**責任與程序** 是否有建立管理職責與程序，確保對資訊安全事故迅速、有效及有條理的回應。				
A.16.1.2	**通報資訊安全事件** 是否有循適當的管理管道儘快通報資訊安全事件。				
A.16.1.3	**通報資訊安全弱點** 是否有要求資訊系統與服務的所有受僱人員、承包商及第三方使用者記錄與通報明顯的或可疑的系統或服務之任何安全弱點。				
A.16.1.4	**資訊安全事件的評鑑與決定** 是否評鑑資訊安全事件，並決定是否歸類為資訊安全事故。				
A.16.1.5	**對資訊安全事故的回應** 是否依據文件化程序對資訊安全事故作回應。				
A.16.1.6	**從資訊安全事故中學習** 是否有適當的機制使資訊安全事故的類型、數量及成本能被量化與監控。				
A.16.1.7	**證據的收集** 資訊安全事故後，對人或組織的跟催行動涉及法律行動（不是民事就是刑事）時，證據的收集、保留及提交是否有符合證據規則，以在相關審判時提出。				
A.17	**營運持續管理的資訊安全層面**				
A.17.1	**資訊安全的持續性** 是否有建立對應方法或程序以防治營運活動的中斷，保護重要營運過程不受重大資訊系統失效或災害的影響，並確保及時的回復。				
A.17.1.1	**規劃資訊安全的持續性** 是否有發展與實作計畫，以在重要營運過程中斷或失效後，維持或恢復作業；並確保資訊在必要時間內達到所要求等級的可用性。				
A.17.1.2	**實施資訊安全持續** 是否有發展與維護全組織持續營運的管理過程，處理組織持續營運所需的資訊與資訊安全要求。 是否有發展與實作計畫，以在重要營運過程中斷或失效後，維持或恢復作業；並確保				

開南大學
KAINAN University

章節	稽核要點	稽核結果			稽核發現
		符合	不符合	不適用	
	資訊在必要時間內達到所要求等級的可用性。 是否有維持單一營運持續計畫之框架，以確保所有計畫皆一致、一貫地處理資訊安全要求，並識別測試及維護的優先順序。				
A.17.1.3	**驗證、審查及評估資訊安全持續** 營運持續計畫是否有定期測試與更新，以確保維持最新且有效。				
A.17.2	**複式配置** 是否確保資訊處理設施的可用性。				
A.17.2.1	**資訊處理設施的可用性** 資訊處理設施是否有足夠的複式配置，以符合可用性要求。				
A.18	**遵循性**				
A.18.1	**遵循適法性與契約要求** 是否有建立對應方法或程序以避免違反任何法律、行政命令、管理規定或合約義務，以及任何安全要求。				
A.18.1.1	**識別適用之法規與契約要求** 對組織與每一資訊系統，是否有明確界定、文件化、並維持最新所有與資訊系統有關之法規、管理規定及合約要求，與組織滿足上述要求的方法。				
A.18.1.2	**智慧財產權** 是否有實作適當流程，以確保關於可能有智慧財產權及專屬軟體產品資料的使用上遵守法令的、管理規定的及合約的要求。				
A.18.1.3	**紀錄的保護** 是否有依據法令的、管理規定的、合約的及營運的要求保護重要記錄，以防止遺失、毀損及偽造。				
A.18.1.4	**隱私權與個人識別資訊的保護** 是否有如相關法令、管理規定及若適用合約條款所要求的，確保資料保護與隱私。				
A.18.1.5	**密碼控制措施的規定** 是否有依照所有相關的協議、法律及管理規定使用密碼控制措施。				
A.18.2	**資訊安全審查** 是否確保資訊安全是依據組織政策與程序實施與操作。				
A.18.2.1	**資訊安全的獨立審查** 是否有實施定期或當安全實作發生重大變更時，獨立審查組織管理資訊安全的方法與				

開南大學
KAINAN University

章節	稽核要點	稽核結果			稽核發現
		符合	不符合	不適用	
	其實作（例如：資訊安全的控制目標、控制措施、政策、過程及程序）。				
A.18.2.2	**安全政策與標準的遵循性** 管理者是否有確保其責任範圍內所有安全程序皆正確執行，以達到遵循安全政策與標準。				
A.18.2.3	**技術遵循性檢查** 是否有定期核對資訊系統是否遵循安全實作標準。				