XXXXXXX 股份有限公司

資訊安全管理系統

資訊安全稽核檢核表

稽 核 員：_____

聯絡電話：_____

E-Mail：_____

填表日期：中華民國__年__月__日

稽核檢核表

年度：

受稽單位：　　流水號：

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
0	**資通安全管理制度**	**CNS27001 本文**					
0.1	組織是否藉由判定內部及外來的議題來達成資訊安全管理系統所要達到的目的?	4.1 瞭解組織及其全景					
0.2	是否鑑別關注方之需求與期望?	4.2 瞭解關注方之需要及期望					
0.3	主管機關、法令、法規及合約針對資訊安全管理系統的要求包括哪些？	4.2 瞭解關注方之需要及期望					
0.4	與組織相關連的內/外部議題是否已納入資訊安全管理系統的範圍內?	4.3 決定資訊安全管理系統之範圍					
0.5	主管機關、法規、內部主管等對於資訊安全管理系統所提出的要求是否皆已納入此系統的範圍?	4.3 決定資訊安全管理系統之範圍					
0.6	組織與其它組織之間的業務往來是否皆依照此系統的規範納入範圍內？	4.3 決定資訊安全管理系統之範圍					
0.7	資訊安全管理系統之範圍是否書面化?	4.3 決定資訊安全管理系統之範圍					
0.8	組織之資訊安全管理系統是否已依照 ISO27001 國際標準建置及實施?	4.4 資訊安全管理系統					
0.9	每年是否持續改進此系統?	4.4 資訊安全管理系統					
0.10	資訊安全管理系統的政策與目標是否與組織的策略方向相符？	5.1 領導及承諾					
0.11	是否將資訊安全管理系統的要求整合進組織本身的營運流程裡?	5.1 領導及承諾					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
0.12	是否配置建立資訊安全管理系統所需之相關資源？	5.1 領導及承諾					
0.13	高階主管是否有向全組織傳達符合資訊安全目標與遵守資訊安全政策的重要性，以及在法律與持續改進需求下之權責？	5.1 領導及承諾					
0.14	資訊安全管理系統是否有達到預期的結果?	5.1 領導及承諾					
0.15	高階主管是否有指引並支持人員對資訊安全管理系統的有效性做出貢獻？	5.1 領導及承諾					
0.16	高階主管訂定之資訊安全政策是否適用並符合組織的目的?	5.2 政策					
0.17	此政策是否包括資訊安全目標或提供設定其目標之架構?	5.2 政策					
0.18	是否承諾將滿足資訊安全所需及適用的要求？	5.2 政策					
0.19	是否承諾資訊安全管理系統將會持續改進？	5.2 政策					
0.20	資訊安全政策是否皆已書面化?	5.2 政策					
0.21	是否在組織內溝通及傳遞資訊安全政策?	5.2 政策					
0.22	當需要時，資訊安全政策是否能被主管機關、下屬機關、內部人員或廠商取用?	5.2 政策					
0.23	是否能確保資訊安全管理系統符合 ISO27001 國際標準的要求，並明訂內部溝通和指定職責角色與權限？	5.3 組織角色、責任及權限					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
0.24	是否有指派人員針對資訊安全管理系統進行執行績效的報告？	5.3 組織角色、責任及權限					
0.25	組織是否能確保資訊安全管理系統能達成其預期成果?	6.1 因應風險及機會之行動					
0.26	是否採取行動以降低或預防衝擊？	6.1 因應風險及機會之行動					
0.27	資訊安全管理系統是否進行持續改進?	6.1 因應風險及機會之行動					
0.28	組織是否規畫說明風險和機會?	6.1 因應風險及機會之行動					
0.29	是否有規畫如何整合與實施這些活動在資訊安全管理系統的流程中?	6.1 因應風險及機會之行動					
0.30	是否有規畫如何評估這些活動的有效性?	6.1 因應風險及機會之行動					
0.31	組織是否已定義資訊安全風險評鑑流程? 是否已建立可接受之資訊安全風險準則?	6.1 因應風險及機會之行動					
0.32	組織是否已建立資訊安全風險評鑑準則?	6.1 因應風險及機會之行動					
0.33	資訊安全風險評鑑是否可重覆產出一致性、有效性及可比較的結果?	6.1 因應風險及機會之行動					
0.34	是否可於資訊安全管理系統範圍內的資訊識別出資訊安全的風險? 是否可用風險評鑑流程來識別因資訊安全管理系統風險的機密性、完整性及可用性所造成的損失?	6.1 因應風險及機會之行動					
0.35	是否可於資訊安全管理系統範圍內的資訊識別出資訊安全風險的責任歸屬(例如:識別風險擁有者)?	6.1 因應風險及機會之行動					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
0.36	是否可依據識別出的風險分析出資產潛在的衝擊?	6.1 因應風險及機會之行動					
0.37	是否可依據識別出的風險分析出風險實際發生的機率?	6.1 因應風險及機會之行動					
0.38	是否可依據識別出的風險分析及定義風險等級?	6.1 因應風險及機會之行動					
0.39	是否可依據風險準則評估及比較風險分析結果?	6.1 因應風險及機會之行動					
0.40	是否可將已分析之風險排列優先順序?	6.1 因應風險及機會之行動					
0.41	所有資訊安全風險評鑑相關之流程是否皆已書面化?	6.1 因應風險及機會之行動					
0.42	是否已選用適合組織的資訊安全風險處理流程及選項?	6.1 因應風險及機會之行動					
0.43	是否已定義在實施風險處理計畫中的所有控制措施?	6.1 因應風險及機會之行動					
0.44	是否將控制措施之定義與附錄 A 比較，並且識別出不選用的控制措施?	6.1 因應風險及機會之行動					
0.45	適用性聲明是否包含所有的控制措施，並描述適用與不適用的理由?	6.1 因應風險及機會之行動					
0.46	是否制訂資安風險處理計畫?	6.1 因應風險及機會之行動					
0.47	資安風險處理計畫及殘餘風險是否取得風險擁有者的核可?	6.1 因應風險及機會之行動					
0.48	所有資訊安全風險處理相關之流程是否皆已書面化?	6.1 因應風險及機會之行動					
0.49	資訊安全目標是否與其政策一致?	6.2 資訊安全目標及其達成之規劃					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
0.50	資訊安全目標是否可被測量?	6.2 資訊安全目標及其達成之規劃					
0.51	資訊安全目標是否有考量到適用的資訊安全需求和風險評鑑與風險處理的結果?	6.2 資訊安全目標及其達成之規劃					
0.52	資訊安全目標是否能被溝通?	6.2 資訊安全目標及其達成之規劃					
0.53	資訊安全目標是否能適時的被更新?目標是否有書面化?	6.2 資訊安全目標及其達成之規劃					
0.54	為達成資訊安全目標，組織是否有決定需進行哪些作業?	6.2 資訊安全目標及其達成之規劃					
0.55	為達成資訊安全目標，組織是否有決定需要哪些資源?	6.2 資訊安全目標及其達成之規劃					
0.56	為達成資訊安全目標，組織是否有決定誰需負責?	6.2 資訊安全目標及其達成之規劃					
0.57	為達成資訊安全目標，組織是否有決定何時需完成計畫中的工作項目?	6.2 資訊安全目標及其達成之規劃					
0.58	為達成資訊安全目標，組織是否有決定結果應如何評估?	6.2 資訊安全目標及其達成之規劃					
0.59	為建立、實施、維持及持續改進資訊安全管理制度，組織是否提供所需的資源?	7.1 資源					
0.60	組織是否有管控執行資訊安全管理制度之人員所需的能力?	7.2 能力					
0.61	組織是否依據其適當之教育訓練和經驗來確定相關作業人員的能力?	7.2 能力					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
0.62	在適用時，組織是否採取行動（例如:實務指導、現職人員轉任、或聘僱能勝任工作的人員）以取得必要之能力，並評估行動的有效性?	7.2 能力					
0.63	組織是否保留適當之書面化資料以作為達到能力的證據?	7.2 能力					
0.64	組織控管下執行工作之人員是否具備資訊安全政策之認知?	7.3 認知					
0.65	人員是否對資訊安全管理制度之有效性及利益具有相關認知?	7.3 認知					
0.66	人員是否有對不符合資訊安全管理制度所隱含之結果有相對的認知?	7.3 認知					
0.67	組織是否決定與資訊安全管理制度之內外部溝通的需求，並了解需進行溝通的項目?	7.4 溝通或傳達					
0.68	組織是否決定需與內外部進行溝通內容的時間點?	7.4 溝通或傳達					
0.69	組織是否決定並了解需要進行內外部溝通的對象?	7.4 溝通或傳達					
0.70	組織是否決定何人來進行與內外部溝通資訊安全管理制度的相關事宜?	7.4 溝通或傳達					
0.71	資訊安全管理制度是否包括 ISO27001 國際標準要求之書面化資料?	7.5 文件化資訊					
0.72	資訊安全管理制度是否包括決定有效性所需之書面化資料?	7.5 文件化資訊					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
0.73	當建立與更新書面資料時，是否確保適當的鑑別與描述（例如:抬頭、日期、製作者或參考號碼)?	7.5 文件化資訊					
0.74	當建立與更新書面資料時，是否確保適當的格式(例如:語言、軟體版本、圖解）與媒體（例如:紙本、電子檔)?	7.5 文件化資訊					
0.75	當建立與更新書面資料時，是否確保適當及適切性的審查與核准?	7.5 文件化資訊					
0.76	資訊安全管理制度所要求的書面化資料當時/地需要時，是否可取得以利使用?	7.5 文件化資訊					
0.77	資訊安全管理制度所要求的書面化資料是否已適當的保護（例如:防止機密外洩、不適當的使用、或喪失完整性)?	7.5 文件化資訊					
0.78	書面資料是否分發使其可取用?	7.5 文件化資訊					
0.79	書面資料之管控單位是否會闡述如何儲存與防護?	7.5 文件化資訊					
0.80	書面資料之管控單位是否會闡述如何變更管控(如版本變更)?	7.5 文件化資訊					
0.81	書面資料之管控單位是否會闡述如何保存與屆期處置?	7.5 文件化資訊					
0.82	外來書面資料為資訊安全管理制度之規劃與運作所需時，是否適當的進行鑑別與管控?	7.5 文件化資訊					
0.83	組織是否藉由規劃、實施與管控所需之流程來滿足資訊安全管理制度的要求?	8.1 運作之規劃及控制					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
0.84	是否實施風險評鑑與處理之相關活動?	8.1 運作之規劃及控制					
0.85	組織是否實施計畫以達成資訊安全目標與規劃?	8.1 運作之規劃及控制					
0.86	組織是否針對發包或委外流程進行管控?	8.1 運作之規劃及控制					
0.87	組織是否於規劃 ISMS 期間建立資訊安全風險評鑑?	8.2 資訊安全風險評鑑					
0.88	當組織運作有異動時是否適時的調整實施的準則?	8.2 資訊安全風險評鑑					
0.89	組織是否將風險評鑑結果書面化?	8.2 資訊安全風險評鑑					
0.90	是否妥善保留其書面化資料?	8.2 資訊安全風險評鑑					
0.91	組織是否有實施資訊安全風險處理計畫?	8.3 資訊安全風險處理					
0.92	組織是否妥善的保留資訊安全處理計畫之書面化結果?	8.3 資訊安全風險處理					
0.93	組織是否有評估資訊安全績效及 ISMS 的有效性?(如何評估?指派誰去評估？)	9.1 監控、測量、分析及評估					
0.94	組織是否決定需進行監控及量測的項目?	9.1 監控、測量、分析及評估					
0.95	組織如何決定監控、測量、分析與評估的方法以確保結果的有效性?	9.1 監控、測量、分析及評估					
0.96	組織何時執行監控與測量?	9.1 監控、測量、分析及評估					
0.97	組織指派何人進行監控與測量?	9.1 監控、測量、分析及評估					
0.98	組織何時進行監控及測量結果的分析與評估?	9.1 監控、測量、分析及評估					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
0.99	組織是否決定指派何人進行結果的分析與評估?	9.1 監控、測量、分析及評估					
0.100	組織是否在規定期間執行內部稽核?(何時執行內稽? 多久執行一次? 由誰來執行內稽?)	9.2 內部稽核					
0.101	定期執行內部稽核是否可符合組織本身對 ISMS 之要求?定期執行內部稽核是否可符合 ISO27001 國際標準之要求?	9.2 內部稽核					
0.102	定期執行內部稽核是否可有效的實施與維持 ISMS?	9.2 內部稽核					
0.103	組織是否有規劃、建立、實施與維持內部稽核的方案 (包括執行的頻率、方法、職責分配、規劃要求與報告)? 稽核方案是否有將相關流程及之前稽核結果入考量?	9.2 內部稽核					
0.104	組織是否有訂定每次稽核之稽核準則與範圍?	9.2 內部稽核					
0.105	為確保稽核流程之客觀性與公正性，組織是否慎重的挑選稽核員執行稽核?	9.2 內部稽核					
0.106	組織如何確保稽核的結果有報告相關管理階層?	9.2 內部稽核					
0.107	組織是否妥善的保留稽核計畫與其稽核結果的書面資料作為證據?	9.2 內部稽核					
0.108	為確保資訊安全管理系統持續的適當性和有效性，高階主管是否有在規定期間和有重大變動時對組織的 ISMS 做審查?	9.3 管理審查					
0.109	管理審查是否將之前會議所訂之狀況納入考量?	9.3 管理審查					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
0.110	管理審查是否將 ISMS 內外部議題的變動納入考量?	9.3 管理審查					
0.111	管理審查是否將 ISMS 績效 (例如:不符合事項與矯正行動) 納入考量?	9.3 管理審查					
0.112	管理審查是否將 ISMS 績效 (例如:監控與量測評估結果) 納入考量?	9.3 管理審查					
0.113	管理審查是否將 ISMS 績效 (例如:稽核結果) 納入考量?	9.3 管理審查					
0.114	管理審查是否滿足資訊安全目標?	9.3 管理審查					
0.115	管理審查是否將利害相關者的回饋納入考量?	9.3 管理審查					
0.116	管理審查是否將風險評鑑與風險處理計畫的結果納入考量?	9.3 管理審查					
0.117	管理審查是否有評估哪些項目是有持續改進的空間?	9.3 管理審查					
0.118	管理審查是否包含相關持續改善機會及改變 ISMS 的需求? 組織是否妥善的保留書面化的管理審查結果證據?	9.3 管理審查					
0.119	當不符合情況時，組織是否對不符合事項做出回應? 1) 採取管控與矯正之行動? 2) 有效處理後果?	10.1 不符合事項及矯正行動					
0.120	是否針對不符合事項有對應的行動，使其不再發生? 1) 審查不符合事項? 2) 判定不符合事項之原因? 3) 決定是否有類似或潛在不符合事項存在?	10.1 不符合事項及矯正行動					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
0.121	當有不符合情況時，組織是否決定及實施所需之矯正行動?	10.1 不符合事項及矯正行動					
0.122	當有不符合情況時，組織是否審查任何矯正行動之有效性?	10.1 不符合事項及矯正行動					
0.123	當有不符合情況並有必要時，組織是否對 ISMS 做出相對應的變動? 矯正行動是否與所遭不符合事項有相對的關連?	10.1 不符合事項及矯正行動					
0.124	當有不符合情況時，組織是否真正了解不符合事項的性質，並採取後續行動? 是否保留書面資料作為證據?	10.1 不符合事項及矯正行動					
0.125	當有不符合情況時，組織是否保留任何矯正行動的書面結果?	10.1 不符合事項及矯正行動					
0.126	組織是否持續改進資訊安全管理制度的適合、適當及有效性?	10.2 持續改進					
5	**資通安全政策訂定與評估**						
5.1	所發佈的資訊安全政策文件是由管理階層核准，是否所有相關使用者可取用？	A.5.1.1 資訊安全政策					
5.2	發佈的資訊安全政策是否定期檢視，若有改變是否仍合宜、適切及有效？	A.5.1.2 資訊安全政策之審查					
6	**資通安全之組織**						
6.1	管理階層是否分派資訊安全相關職責？	A.6.1.1資訊安全之角色及責任					
6.2	是否有明確定義對個別資產之保護及執行特定程序的責任歸屬？	A.6.1.2職務區隔					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
6.3	組織是否和外部相關機關（例如:消防單位、法律施行權威人士、管理團體）保持聯繫？	A.6.1.3與權責機關之連繫					
6.4	組織是否和外部專家(例如：資訊安全專家、資訊安全服務提供者或資訊安全相關團體)保持聯繫，以取得最新的資安相關資訊？	A.6.1.4與特殊關注方之連繫					
6.5	在專案執行過程中是否已將資訊安全納入考量?	A.6.1.5專案管理之資訊安全					
6.6	組織內是否針對行動設備進行資訊安全控管，以避免可能的資訊外漏的風險?	A.6.2.1行動裝置政策					
6.7	從遠端連線登入組織內部系統是否有相對應之政策進行管控，讓內部資訊得以受到保護?	A.6.2.2遠距工作					
7	人力資源安全管理						
7.1	是否在應徵正式、約聘或臨時人員之前，執行驗證檢查及妥當篩選？	A.7.1.1 篩選					
7.2	員工(員工包含正式、約聘或臨時人員)、承包者及第三方使用者是否同意並簽署其聘僱契約之條款與條件，該契約應陳述其與組織對資訊安全的責任？	A.7.1.2 聘用條款及條件					
7.3	管理階層是否有要求員工要遵守資訊安全政策與相關程序？	A.7.2.1 管理階層責任					
7.4	組織是否會定期提供員工(含第三方使用者)資訊安全的相關認知、教育及訓練?	A.7.2.2 資訊安全認知、教育及訓練					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
7.5	員工違反組職之安全政策及程序時，是否有懲處流程？	A.7.2.3 懲處過程					
7.6	是否有明文規範員工調職或離職相關之職責？當員工調職或離職時是否有移除其所使用系統之存取權限？是否有歸還相關資產？	A.7.3.1 聘用責任之終止或變更					
8	資產管理						
8.1	是否製作與資訊系統相關的資產清冊並每年進行盤點、更新，且妥善保管？	A.8.1.1 資產清冊					
8.2	是否針對所有資訊與資產都有分派相對應的人員或單位以保管之？	A.8.1.2 資產擁有權					
8.3	是否針對所有資訊與資產規範其可行的使用方式？	A.8.1.3 資產之可被接受使用					
8.4	所有員工、承包者及第三方使用者在其聘僱、契約或協議終止時，是否歸還其擁有的所有組織資產？	A.8.1.4 資產之歸還					
8.5	組織是否有資訊資產分類程序(例如：依照資訊價值、法令要求、安全性與重要性分級)？	A.8.2.1 資訊之分級					
8.6	組織之資訊資產分類(例如：依照資訊價值、法令要求、安全性與重要性分級）是否正確的標示/標明？	A.8.2.2 資訊之標示					
8.7	針對資訊資產之分享或限制，資產之分類及其相對應之保護控制是否符合公司需求？	A.8.2.3 資產之處置					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
8.8	是否訂定適當的程序以管理儲存資料的物件及可移除式媒體？	A.8.3.1 可移除式媒體之管理					
8.9	組織是否有相關媒體汰除的機制（例如：水銷、銷磁、實體破壞)?	A.8.3.2 媒體之汰除					
8.10	組織針對實體媒體的傳輸過程是否有妥善的保護機制（例如：密封、加密)?	A.8.3.3 實體媒體傳送					
9	存取控制安全						
9.1	資訊存取控制政策是否符合營運及資訊安全要求事項之規定並已書面化？	A.9.1.1 存取控制政策					
9.2	網路與網路應用系統服務的存取是否僅開放給被授權的員工使用，並妥善管理之?	A.9.1.2 對網路及網路服務之存取					
9.3	使用者是否依賦予的權限進行正式帳號的申請、註冊與註銷?	A.9.2.1 使用者註冊及註銷					
9.4	所有的使用者是否依正當管道/流程(依權限)取得或撤銷系統及服務的存取權限?	A.9.2.2 使用者存取權限之配置					
9.5	特殊權限之指派與使用，是否有管制及限制？	A.9.2.3 具特殊存取權限之管理					
9.6	通行碼之分派是否有正式流程控管? 是否遵循安全規範來設定通行碼?	A.9.2.4 使用者之秘密鑑別資訊的管理					
9.7	是否有定期執行使用者存取權限審查之正式流程?	A.9.2.5 使用者存取權限之審查					
9.8	使用者存取權限是否在職務有異動或離職時進行調整或移除?	A.9.2.6 存取權限之移除或調整					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
9.9	是否執行桌面淨空作業或螢幕淨空以避免資料或通行碼未經授權而遭存取、遺失或毀壞？	A.9.3.1 秘密鑑別資訊之使用					
9.10	員工只能直接存取被授權使用之服務? 未經授權的資訊或應用系統功能是否依照存取控制政策加以限制?	A.9.4.1 資訊存取限制					
9.11	當有必要時，存取控制政策是否訂定及提供安全的系統登入流程?	A.9.4.2 保全登入程序					
9.12	是否有通行碼管理制度來確保通行碼/密碼設定的品質?	A.9.4.3 通行碼管理系統					
9.13	是否嚴謹的管控及限制可能會跨(越)權使用之公用程式（例如: 附屬應用程式內的螢幕保護程式、使用者下載不明之Apps/驅動程式)?	A.9.4.4 具特殊權限公用程式之使用					
9.14	是否嚴謹的限制使用者存取程式之原始碼(SOURCE CODE)?	A.9.4.5 對程式源碼之存取控制					
10	密碼學						
10.1	組織是否設有加解密使用及控管之政策來保護資訊?	A.10.1.1 使用密碼式控制措施之政策					
10.2	組織是否設有金鑰使用、保護及有效期限之政策來強化金鑰的管理?	A.10.1.2 金鑰管理					
11	**實體及環境安全**						
11.1	資訊處理設備的實體環境是否受到保護?	A.11.1.1 實體安全周界					
11.2	安全區域是否有適當的進出控制，僅授權的人員可以使用? 是否定期審查並更新進出權限?	A.11.1.2 實體進入控制措施					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
11.3	是否在安全區域實施保護措施以保護辦公室、房間及設備（例如: CCTV)?	A.11.1.3 保全之辦公室、房間及設施					
11.4	是否有實體安控機制以對抗自然或人為的威脅(例如火災、水災、地震、爆破、民運等)?	A.11.1.4 防範外部及環境威脅					
11.5	是否有建立在安全區域內工作之相關程序?	A.11.1.5 於保全區域內工作					
11.6	資訊處理設施是否與一般收發或裝卸區作實體隔離，以避免未經授權之存取？	A.11.1.6 交付及裝卸區					
11.7	設備是否設置好並受保護，以降低環境威脅和危險，以及未經授權存取機會的風險？	A.11.2.1 設備安置及保護					
11.8	設備是否受保護，以避免受支援之公共設施(電力、水力、空調或溫溼度調節器等)故障或其他異常現象干擾？	A.11.2.2 支援之公用服務事業					
11.9	電力和電信電纜在輸送資料或支援資訊服務時，是否受保護，免於被攔截或遭受毀壞？	A.11.2.3 佈纜安全					
11.10	設備是否有定期維護，以確保該設備之可用性與完整性？	A.11.2.4 設備維護					
11.11	針對設備攜出在外地使用是否經由管理者授權？	A.11.2.5 資產之攜出					
11.12	放置於組織場所外之設備與資產是否受到妥善的保護?	A.11.2.6 場所外設備及資產之安全					
11.13	設備在汰除或重新使用前，所有置於儲存設備中的機敏資料是否經確認後刪除或是安全覆蓋以避免資訊不當外洩?	A.11.2.7 設備汰除或再使用之保全					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
11.14	設備無人看管時是否有妥善的防護措施?	A.11.2.8 無人看管之使用者設備					
11.15	組織是否設有桌面清空及螢幕淨空政策，文件及可攜式媒體在人員離開座位時是否受到保護?人員下班及離開時對文件及電腦是否有保護措施?	A.11.2.9 桌面淨空及螢幕淨空政策					
12	**運作安全**						
12.1	資訊處理設備，是否訂有操作程序且已紀錄並被保存？	A.12.1.1 文件化運作程序					
12.2	對於資訊處理設備和系統是否有做變更管理？	A.12.1.2 變更管理					
12.3	容量需求是否受監視，以為未來容量、處理能力和儲存體規劃之依據？	A.12.1.3 容量管理					
12.4	開發、測試及正式運作之環境是否有作隔離？	A.12.1.4 開發、測試及運作環境之區隔					
12.5	使用者針對惡意程式是否有偵測、預防及還原的防護機制，並有相關的認知?	A.12.2.1 防範惡意軟體之控制措施					
12.6	重要業務資訊和軟體是否定期的進行備份?	A.12.3.1 資訊備份					
12.7	使用者於系統上的活動、特例行為、錯誤操作及資訊安全之事件日誌是否有保存，並定期的追蹤及調閱?	A.12.4.1 事件存錄					
12.8	保存日誌之設備與日誌是否有安控機制，以防禦擅自修改或未授權存取？	A.12.4.2 日誌資訊之保護					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
12.9	管理者與操作者於系統上的活動之事件日誌是否有受到安全的保存，並定期的追蹤及調閱?	A.12.4.3 管理者及操作者日誌					
12.10	組織內之所有相關之資訊系統或安全網域的時間是否同步，且依據同一時間來源?	A.12.4.4 鐘訊同步					
12.11	作業系統上的軟體安裝是否符合組織所規定的程序?	A.12.5.1 對運作中系統之軟體安裝					
12.12	組織是否取得最新的資訊安全系統之技術性弱點資訊，組織所暴露的弱點是否被評估且產生相對應措施來處理相關風險?	A.12.6.1 技術脆弱性管理					
12.13	使用者是否有遵守組織內部軟體安裝的限制與規定?	A.12.6.2 對軟體安裝之限制					
12.14	對營運系統的稽核要求和活動是否有謹慎的規劃並取得批准，使營運中斷的損壞和威脅降到最小?	A.12.7.1 資訊系統稽核控制措施					
13	通訊安全						
13.1	網路是否已受到管理及控制來保護系統及應用程式上的資訊?	A.13.1.1 網路控制措施					
13.2	所有網路服務之安全機制、服務層級及管理要求是否已明確的鑑別出來，並包含在網路服務協議中（無論內部或是外包的服務)?	A.13.1.2 網路服務之安全					
13.3	資訊服務、使用者及資訊系統的群組是否在網路中已區隔?	A.13.1.3 網路之區隔					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
13.4	組織是否有正式的傳輸政策、程序及管控措施來保護傳輸中的資訊?	A.13.2.1 資訊傳送政策及程序					
13.5	針對組織與外部機關的業務資訊往來是否訂定資訊傳輸的協議?	A.13.2.2 資訊傳送協議					
13.6	組織內與電子訊息相關之資訊是否受到適當的保護?	A.13.2.3 電子傳訊					
13.7	是否識別與定期審查反映組織對資訊保護之需求的機密性或保密協議要求？	A.13.2.4 機密性或保密協議					
14	**資通系統獲取、開發及維護之安全**						
14.1	在現存資訊系統的加強項目或新系統的業務需求中，是否有加入安控措施的需求？	A.14.1.1 資訊安全要求事項分析及規格					
14.2	在公共網路上的應用程式系統中，資料是否受到保護，以確保資料不被盜用、未經授權揭露或修改?	A.14.1.2 保全公共網路之應用服務					
14.3	應用服務交易中的資訊是否受到保護，以避免不完整傳輸、錯誤路由、未經授權訊息變更/洩露/複製?	A.14.1.3 保護應用服務交易					
14.4	組織內針對軟體和系統開發是否有建立並遵守規範?	A.14.2.1 保全開發政策					
14.5	在開發過程中系統的變更是否皆有效控管，並遵循系統變更控制程序?	A.14.2.2 系統變更控制程序					
14.6	當作業平台變更時，重要業務應用系統是否有審查及測試，以確保組織的營運及安全不會有不利的衝擊?	A.14.2.3 運作平台變更後，應用之技術審查					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
14.7	套裝軟體的修改是否僅針對 “必要時”才可進行，所有的變更皆有嚴謹的控管?	A.14.2.4 軟體套件變更之限制					
14.8	資訊系統的實行否有建立、記錄、維護和運用系統工程的安全規範?	A.14.2.5 保全系統工程原則					
14.9	在整個系統開發的期程內，組織是否建立安全的開發環境供系統開發及整合?	A.14.2.6 保全開發環境					
14.10	組織是否有效的監督委外的系統開發活動及過程?	A.14.2.7 委外開發					
14.11	資訊系統功能的安全性是否在開發過程中有進行測試?	A.14.2.8 系統安全測試					
14.12	當建置新資訊系統和版本更新/升級時，組織是否設定新準則與驗收測試方案?	A.14.2.9 系統驗收測試					
14.13	測試資料是否已嚴謹的篩選、保護及控管?	A.14.3.1 測試資料之保護					
15	**供應者關係**						
15.1	為減緩供應商存取組織資產而衍生的風險，組織是否訂定並書面化相關資訊安全要求及政策?	A.15.1.1 供應者關係之資訊安全政策					
15.2	是否與每個可能存取、處理、儲存組織資訊、與組織通信或為提供 IT 基礎設施之供應商建立並協議所有相關的資訊安全要求?	A.15.1.2 於供應者協議中闡明安全性					
15.3	供應商的資訊安全協議是否包括資訊和通信技術服務以及產品供應鏈相關之資訊安全風險處理要求?	A.15.1.3 資訊及通訊技術供應鏈					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
15.4	組織是否定期的監督、審查和稽核供應商所提供的服務?	A.15.2.1 供應者服務之監視及審查					
15.5	供應商服務的變更（包括維持及改善現有的資訊安全政策、程序和控制措施）是否有考量到重要業務資訊、系統流程和風險的重新評估?	A.15.2.2 管理供應者服務之變更					
16	**資通安全事故管理**						
16.1	是否有規範資訊安全事件管理職責與程序，以迅速且有效地管理資訊安全事件？	A.16.1.1 責任及程序					
16.2	是否循適切的管理管道，儘速通報資訊安全事件？	A.16.1.2 通報資訊安全事件					
16.3	是否要求資訊系統與服務的所有員工、承包者及第三方使用者，注意並通報系統或服務中之任何觀察到或可疑的資訊安全弱點？	A.16.1.3 通報資訊安全弱點					
16.4	針對資訊安全事件，是否有機制來分析和評估，並決定是否歸類為資訊安全事件？	A.16.1.4 對資訊安全事件之評鑑及決策					
16.5	針對資訊安全事件，是否有相對的回應並有書面化的紀錄?	A.16.1.5 對資訊安全事故之回應					
16.6	在經歷過資訊安全事件的衝擊，人員是否有從中學習，並減少未來類似的事件再發生?	A.16.1.6 由資訊安全事故中學習					
16.7	證據的蒐集是否符合相關法律的蒐證規定、特定法院的規定、公告標準或法院判例，以產生可被接受的證據？	A.16.1.7 證據之收集					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
17	**營運持續管理之資通安全層面**						
17.1	是否發展與維持整個組織營運持續的管理過程，以因應組織營運持續所需的資訊安全要求？	A.17.1.1 規劃資訊安全持續					
17.2	是否有根據風險評估結果擬訂營運持續計畫，並識別測試與維護的優先順序，以確保組織資訊安全方面業務持續營運？	A.17.1.2 實作資訊安全持續					
17.3	定期測試營運持續計畫，且透過定期審查來加以維護，以確保這些規劃為最新且有效？當組職的重要業務流程中斷或失效時，是否有既定的計畫以供及時維持或回復業務營運？	A.17.1.3 查證、審查並評估資訊安全持續					
17.4	資訊處理設備是否有備援部署，以滿足可用性之需求?	A.17.2.1 資訊處理設施之可用性					
18	**遵循性**						
18.1	對每一個資訊系統與組織， 所有相關法令、法規與契約要求及組織用以符合此等要求之作法，是否加以明確界定、文件化及維持最新？	A.18.1.1 適用之法規及契約的要求事項之識別					
18.2	是否實施適當的程序，以確保在使用與智慧財產權有關的工具（或資料），及適合的軟體產品時，能遵守相關的法律限制？	A.18.1.2 智慧財產權					
18.3	重要的紀錄是否已加以保護，而不致發生遺失、損毀或偽造等情事？	A.18.1.3 紀錄之保護					

項次	稽核要點	依據標準（CNS27001）	接洽人	稽核結果			稽核發現
				符合	不符合	不適用	
18.4	是否有依據相關法令來保護個人資訊及隱私？	A.18.1.4 個人可識別資訊之隱私及保護					
18.5	是否使用密碼控制措施，以遵循所有相關的協議、法律及法規？	A.18.1.5 密碼式控制措施之監管					
18.6	資訊安全政策之施行過程是否由組織內獨立的單位來檢核？當重大事件發生時，是否有獨立的單位進行審查?	A.18.2.1 資訊安全之獨立審查					
18.7	是否訂有資訊安全內部稽核計畫(含稽核目標、範圍、時間、程序、人員)及產生稽核報告？是否定期審查範圍內之安全處理及程序的遵循性?	A.18.2.2 安全政策及標準之遵循性					
18.8	資訊系統是否定期檢視以符合安全建置標準？	A.18.2.3 技術遵循性審查					