

稽核人員 田均開

達和環保服務股份有限公司

資通安全管理內部稽核查檢表

章節與說明	符合度				稽核發現
6 規劃					
6.1.2 資通安全風險評鑑	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	缺表單 適用性聲明書 資通系統清冊 資訊安全等級評估表 資通威脅及弱點評估表
組織應界定與應用資通安全風險評鑑流程以： a) 建立與維護資通安全風險準則，包含： 1) 風險接受準則； 2) 決定執行資通安全風險評鑑的準則； b) 確保重複執行的資通安全評鑑能產生一致、有效並可比較的結果。 c) 識別資通安全風險： 1) 應用資通安全風險評鑑流程來識別 ISMS 範圍中與資訊機密性、完整性與可用性喪失相關的風險。 2) 識別風險擁有者。 d) 分析資通安全風險： 1) 評估在 6.1.2 c 1) 已識別風險可能產生的潛在結果； 2) 評估在 6.1.2 c 1) 已識別風險發生真正的可能性； 3) 決定風險的等級； e) 評估資通安全風險： 1) 將風險分析結果與 6.1.2 a) 建立的風險準則進行比較分析； 2) 為分析的風險排列風險處理的優先順序。					
8 運作					
8.2 資訊安全風險評鑑	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	有風險評鑑表
組織應定期或於預訂或執行重大變更時，執行風險評鑑，並考量 6.1.2 a) 所建立的準則。 組織應保存資訊安全風險評鑑結果的文件化資訊。					

達和環保服務股份有限公司
資通安全管理內部稽核查檢表

章節與說明	符合度				稽核發現
A. 8 資產管理					
A. 8.1 資產責任					
A. 8.1.1 資產清冊 資訊與資訊處理設施相關的資產應加以識別，該資產清單應加以製作與維護。	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	盈利=資產清單表
A. 8.1.2 資產的擁有權 資產清冊中維護的資產應有擁有者。	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	同上
A. 8.1.3 資產之可被接受的使用 資訊與資訊處理設施相關的資訊與資產，其可被接受的使用之規則應予以識別、文件化及實作。	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	由本機電腦設備識別
A. 8.1.4 資產歸還 所有員工與外部團體使用者在其聘僱、契約或協議終止時，應歸還其擁有的所有組織資產。	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	歸還職工繳回電腦設備
A. 8.2 資訊分級					
A. 8.2.1 分級資訊 資訊應依其對未經授權的揭露或修改的法律要求、價值、重要性及敏感性加以分類。	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	公開訊息聲明 分為四級：一般、限閱、敏感、机密
A. 8.2.2 資訊標示 應依照組織所採用的分類法，發展與實作一套適當的資訊標示程序。	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input checked="" type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	資訊資產分七類。 硬件及通訊設備：無標示重 要等級及財產標示

達和環保服務股份有限公司
資通安全管理內部稽核查檢表

<p>A.8.2.3 資產處置 ✓</p> <p>應依照組織所採用的分類法，發展與實作一套適當的資產處置程序。</p>	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	<p>1. 資訊設備汰除，其儲存元件 另外拆下來，破壞銷毀 2. 依公司程序進行報廢</p>
<p>A.8.3 媒體處置</p>					
<p>A.8.3.1 可移除式媒體的管理</p> <p>應依照組織所採用的分類法，實作可移除式媒體管理程序。</p>	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	<p>USB 執行程式管制</p>
<p>A.8.3.2 媒體的汰除 ✓</p> <p>媒體不再需要時，應使加以安全地汰除。</p>	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	
<p>A.8.3.2 實體媒體輸送</p> <p>應保護含有資訊的媒體在傳輸時，避免未經授權的存取、誤用或毀損。</p>	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	<p>須驗證方可連線</p>

周金平

張山

達和環保服務股份有限公司
資通安全管理內部稽核查檢表

章節與說明	符合度				稽核發現				
A. 9 存取控制									
A. 9.1 存取控制之營運要求									
A. 9.1.1 存取控制政策 應基於營運與資訊安全要求，建立、文件化及審查存取控制政策。	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input checked="" type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	檔案伺服器文件存取權限應釐清並定期審查				
A. 9.1.2 網路與網路服務存取 應僅提供使用者經特定授權可存取的網路與網路服務。	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	總登入透過AD驗證或是系統權限驗證				
A. 9.2 使用者存取管理									
A. 9.2.1 使用者註冊與註銷註冊 正式的使用者註冊與註銷註冊流程應加以實作，以確保存取權限的指派。	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	AD帳號變動ERP異動單				
A. 9.2.2 使用者存取提供 正式使用者存取提供流程應加以實作，以指派或撤銷所有系統與服務之各項使用者類別的存取權限。	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	依異動單調整				
A. 9.2.3 特殊存取權限管理 應限制與控制特權的配置與使用。	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	一般同仁限制USER權限資訊管理人員另外建管理帳號				
A. 9.2.4 使用者秘密鑑別資訊的管理 秘密授權資訊的配置應透過正式管理流程加以控制。	<input type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input checked="" type="checkbox"/> 不適用					

駱心亭

達和環保服務股份有限公司
資通安全管理內部稽核查檢表

A. 9.2.5 使用者存取權限的審查	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	定期審查使用者帳號、ERP使用者權限檢視
資產擁有者應定期審查使用者存取權限。					
A. 9.2.6 存取權限的移除或調整	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	依異動單據調整刪除
所有員工與外部團體使用者對資訊及資訊處理設施的存取權限，在其聘僱、合約或協議終止時，或因變更而調整時，均應予以移除。					
A. 9.3 使用者責任					
A. 9.3.1 秘密鑑別資訊的使用	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	防火牆、網站、使用加密金鑰登入
應要求使用者於使用秘密授權資訊時，遵循組織實務。 通行碼加密鎖鑰憑証					
A. 9.4 系統與應用程式存取控制					
A. 9.4.1 資訊存取限制	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	
應根據存取控制政策，限制對資訊與應用系統功能之存取。					
A. 9.4.2 保全登入資訊	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	限定須由跳板機登入廠商
當有存取控制政策要求時，應由保全登入程序來控制系統與應用程式的存取。					
A. 9.4.3 通行碼管理系統	<input type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input checked="" type="checkbox"/> 不適用	
管理通行碼的系統應為互動式，並應確保通行碼嚴謹。					
A. 9.4.4 特權公用程式的使用	<input type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input checked="" type="checkbox"/> 不適用	
可能篡越系統與應用控制措施的公用程式之使用，應加以限制與嚴密控制。					

達和環保服務股份有限公司
資通安全管理內部稽核查檢表

A. 9. 4. 5 程式源碼的存取控制	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
應用程式的原始碼的存取應加以限制。	符合	建議事項	不符合	不適用	

路達 監核

達和環保服務股份有限公司
資通安全管理內部稽核查檢表

章節與說明	符合度				稽核發現
A.10 密碼措施					
A.10.1 密碼控制措施					
A.10.1.1 使用密碼控制措施的政策	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
使用密碼控制措施以保護資訊的政策應加以發展與實作。	符合	建議事項	不符合	不適用	
A.10.1.2 金鑰管理	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	SSL憑証
加密金鑰使用、保護與存續期間的政策，應加以發展與實作於整個生命週期。	符合	建議事項	不符合	不適用	

王維民

張連

達和環保服務股份有限公司
資通安全管理內部稽核查檢表

章節與說明	符合度				稽核發現				
A.12 作業安全									
A.12.1 作業程序與責任									
A.12.1.1 文件化作業程序 ✓ 作業程序應加以文件化，並讓所有需要的使用者均可隨時取得。	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	存放檔案伺服器內				
A.12.1.2 變更管理 影響資訊安全的組織、營運流程、資訊處理設施與系統變更應加以控制。	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用					
A.12.1.3 容量管理 各項資源的使用應加以監視、調諧(tune)，並對未來容量要求預作規劃，以確保所要求的系統效能。	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	NAS 可擴充儲存容量的硬碟櫃				
A.12.1.4 開發、測試及運作環境的分隔 開發、測試及運作之環境應加以分隔，以降低對運作之環境未經授權存取或變更的風險。	<input type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input checked="" type="checkbox"/> 不適用					
A.12.2 防範惡意碼									
A.12.2.1 惡意碼的控制措施 防範惡意碼的偵測、預防及復原控制措施，應加實作，並應結合適切的使用者認知。	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	Crowstrike 監控				
A.12.3 備份									
A.12.3.1 資訊備份 ✓ 應依據所議定的備份政策，定期進行資訊、軟體與系統影像檔的備份與測試。	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	Acronis 保留一週五天，四週-6月。				

達和環保服務股份有限公司
資通安全管理內部稽核查檢表

A. 12.4 存錄與監視						
A. 12.4.1 事件存錄		<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	AD系統事件記錄 Vcenter系統記錄
事件存錄係記錄使用者活動、例外情形、錯誤及資訊安全事件，應加以產生、保存並定期審查。 <i>log</i>						
A. 12.4.2 日誌資訊的保護		<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	定期備份系統
存錄設施與日誌資訊應加以保護，以避免竄改與未經授權的存取。						
A. 12.4.3 管理者與操作者日誌		<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	FW 登入記錄 定期存檔
系統管理者與操作者的活動應加以存錄、保護及定期審查。						
A. 12.4.4 鐘訊同步		<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	NTP 設置同步
組織或安全領域內所有相關資訊處理系統的鐘訊，應與單一參考時間來源同步。						
A. 12.5 作業軟體的控制						
A. 12.5.1 作業系統上的軟體安裝		<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	EDR 控管
應實作程序來控制作業系統上的軟體安裝。						
A. 12.6 技術脆弱性管理						
A. 12.6.1 技術脆弱性管理 <i>弱點</i>		<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	定期掃描
應及時取得關於使用中資訊系統的技術脆弱性資訊、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。						

達和環保服務股份有限公司
資通安全管理內部稽核查檢表

A. 12. 6. 2 軟體安裝的限制 ✓	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	只有管理有權安裝
使用者軟體安裝的管理規則應加以建立與實作。					
A. 12. 7 資訊系統稽核的考量					
A. 12. 7. 1 資訊系統稽核控制	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	有公告，不影響營運。
有關作業系統查核的稽核要求與活動，應謹慎規劃及議定，使營運過程中斷之風險降至最低。					


 駱心遠

達和環保服務股份有限公司
資通安全管理內部稽核查檢表

章節與說明	符合度				稽核發現				
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	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	特定組段有存取權限系統				
網路應適切地加以管理與控制，以保護系統與應用程式的資訊。									
A. 13.1.2 網路服務的安全	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	簽訂維護合約 約定服務水準				
所有網路服務的安全機制、服務水準及管理要求，應加以識別並納入網路服務協議中，不論是此等服務是由內部或委外所提供。									
A. 13.1.3 網路區隔	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	使用者只能存取權限由系統				
資訊服務、使用者及資訊系統各群組使用的網路應加以區隔。									
A. 13.2 資訊轉移									
A. 13.2.1 資訊轉移政策與程序	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input checked="" type="checkbox"/> 不適用	IT人員協助設備連接，由使用者自行轉移，確保可復原回轉移前的狀態				
應備妥適當的正式轉移政策、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轉移。									
A. 13.2.2 資訊轉移協議	<input checked="" type="checkbox"/> 符合	<input type="checkbox"/> 建議事項	<input type="checkbox"/> 不符合	<input type="checkbox"/> 不適用	合約協議 轉移步驟及資料保護、復原流程				
組織與外部團體間協議應說明安全的營運資訊轉移。									

達和環保服務股份有限公司
資通安全管理內部稽核查檢表

A. 13. 2. 3 電子傳訊	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Office 365 系統保護
電子傳訊涉及的資訊應適當地加以保護。	符合	建議事項	不符合	不適用	
A. 13. 2. 4 機密性或保密協議	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	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，應加以識別、定期審查與文件化	符合	建議事項	不符合	不適用	

張峰