



大 仁 科 技 大 學
T a j e n U n i v e r s i t y

管 制 文 件 訂 修 廢 履 歷 表

文件編號		資訊-程序-06	文件名稱	資訊安全風險管理程序書		
使用部門		圖書資訊館			機密等級	普通
版次	頁數	文件修訂摘要				實施日期
A.0	7	初版				99/05/24
B.0	7	修正「資訊-程序-06-01 風險評鑑工作表、資訊-程序-06-02 風險處理計畫表、資訊-程序-06-04 殘餘風險評鑑工作表」三張表單，增加審核機制。				99/08/12
訂修廢者			單位主管		資訊安全長	

※管制文件不得擅自塗改及做記號並禁止影印。

資訊-程序-01-02A 普通



1.目的

為使本校之資訊資產風險評鑑與處理作業有一明確規範，以鑑別資訊資產之弱點及威脅而導致之風險，並依據評鑑結果採取對策或控制措施，降低資訊資產遭受損害的風險，特制定本程序書。

2.適用範圍

凡本校資訊安全風險管理之作業，均適用本程序書。

3.參考文件

3.1 資訊-程序-04 資訊資產管理程序書。

3.2 資訊-標準-03 資訊安全風險評鑑量化表。

4.名詞定義

4.1 風險 (Risk)

威脅會利用資產的弱點造成資產的損失或損壞的潛在可能性。

4.2 威脅 (Threat)

資訊資產所面臨的事件，可能會對系統或組織及其資產造成傷害，威脅必須利用資產的弱點才能對資產造成傷害。

4.3 弱點 (Vulnerability)

指單一或一系列會讓威脅有機可趁而造成資產損害的狀況。資產的脆弱點本身並不會造成傷害。

4.4 風險管理 (Risk management)

以可接受的成本，對可能影響資訊資產的安全風險進行鑑別、控制及降低或排除的過程。包含風險評鑑與風險處理。

4.5 風險評鑑 (Risk assessment)

對資訊資產及資訊處理設施的威脅、衝擊及弱點及其發生可能性的評鑑。

4.6 風險處理 (Risk treatment)

選擇與實施各項控制措施，以修正風險的過程。

4.7 資產價值 (資產鑑定 C、I、A)



4.7.1 機密性 (Confidentiality, 簡稱 C): 確保只有經過授權的人才能存取資訊。

4.7.2 完整性 (Integrity, 簡稱 I): 保護資訊及其處理方法的準確性和完整性。

4.7.3 可用性 (Availability, 簡稱 A): 確保經過授權的使用者在需要時可以存取資訊並使用相關資訊資產。



5.作業內容

5.1 資訊安全風險管理流程圖

流程	權責	相關文件
產生風險評鑑需求	資訊安全工作小組	
↓		
建立風險評鑑方法	資訊安全工作小組	
↓		
資訊資產鑑別與評價	資訊安全工作小組	資訊資產清冊
↓		
弱點及威脅分析	資訊安全工作小組	風險評鑑工作表
↓		
計算風險值	資訊安全工作小組	風險評鑑工作表
↓		
撰寫風險評鑑報告	資訊安全工作小組	風險評鑑報告
↓		
決定可接受風險等級	資訊安全執行小組	風險評鑑報告
↓		
擬定及執行 風險處理計畫	資訊安全工作小組	風險處理計畫表
↓		
評估風險 處理執行成效	資訊安全執行小組	殘餘風險評鑑工作表
↓		
紀錄保存	資訊安全工作小組	



5.2 產生風險評鑑需求

風險評鑑作業應每年定期執行，並由資訊安全工作小組決定執行之時機與範圍。除每年定期執行外，亦應於下列情形發生時，針對變動範圍內的作業程序與資訊資產進行風險評鑑：

5.2.1 營運組織變更

5.2.2 作業流程改變

5.2.3 資訊資產新增或變更

5.2.4 發生重大資訊安全事件

5.3 建立風險評鑑方法

5.3.1 風險評鑑因素

風險評鑑為計算資訊資產風險值之程序，用以決定風險處理之優先順序。資訊資產風險值是以其機密性、完整性、可用性等三項因子所構成之資訊資產價值，以及資訊資產所面臨之弱點脆弱度與威脅發生機率決定。

5.3.2 風險值計算流程

根據風險評鑑表格進行資訊資產評價，識別弱點之脆弱度、威脅之發生機率，將此三項評分進行相乘，並依威脅對機密性、完整性、可用性所造成之衝擊影響進行風險值加總，即求出該資訊資產之風險值。

5.3.3 風險值公式

風險值因子	代號
資產價值之機密性	C
資產價值之完整性	I
資產價值之可用性	A
機密性之衝擊影響	CI
完整性之衝擊影響	II
可用性之衝擊影響	AI
弱點脆弱度	V
威脅發生機率	T

5.3.4 資訊資產總風險值 = $\{(CI \times V \times T \times C) + (II \times V \times T \times I) +$



(AI×V×T×A)}

5.4 資訊資產鑑別與評價

5.4.1 資訊資產鑑別

資訊安全工作小組依據「資訊-程序-04 資訊資產管理程序書」之作業說明，執行資訊資產鑑別作業，並建立「資訊-程序-04-01 資訊資產清冊」。建立資訊資產清冊之作業方式詳見「資訊-程序-04 資訊資產管理程序書」。

5.4.2 資訊資產評價

資訊資產管理者須針對各項資訊資產之機密性、完整性、可用性等三項資訊資產價值因子進行資訊資產評價。各因子評價標準應依據「資訊-標準-03 資訊安全風險評鑑量化表」中「資訊資產評價」章節對資訊資產進行評價。

5.5 弱點及威脅分析

5.5.1 資訊資產管理者須針對各項資訊資產之使用及管理現狀，識別資訊資產所面臨之內部弱點及外在威脅，並分析其脆弱度與發生機率。

5.5.2 資訊資產弱點之識別應依據「資訊-標準-03 資訊安全風險評鑑量化表」中「資訊資產之弱點、威脅與衝擊對應表」內之對應關係，列出各項資訊資產可能之弱點。

5.5.3 資訊資產威脅之識別應依據「資訊-標準-03 資訊安全風險評鑑量化表」中「資訊資產之弱點、威脅與衝擊對應表」內之對應關係，列出各項資訊資產弱點所存在之可能威脅。

5.5.4 依據「資訊-標準-03 資訊安全風險評鑑量化表」中「資訊資產之弱點、威脅與衝擊對應表」，鑑別各項威脅對資訊資產所造成之機密性、完整性、可用性之衝擊。

5.5.5 根據 5.5.2、5.5.3、5.5.4 作業，將資訊資產清冊、資訊資產評價整合，建立「資訊-程序-06-01 風險評鑑工作表」。

5.5.6 資訊資產管理者依「資訊-程序-06-01 風險評鑑工作表」，針對資訊資產弱點之脆弱度（「弱點評估-脆弱度」欄）及威脅之發生機率（「威脅評估-發生機率」欄）進行評分。評分標



準分別詳見「資訊-標準-03 資訊安全風險評鑑量化表」中「資訊資產弱點脆弱度評分」及「資訊資產威脅發生機率評分」。

5.6 計算風險值

根據「資訊-程序-06-01 風險評鑑工作表」所評鑑之資產價值（「營運衝擊評估」欄）、弱點（「弱點評估」欄）及威脅（「威脅評估」欄）分析，依本說明書 5.3.4 之計算公式進行風險值之計算，以獲得資訊資產之總風險（「風險值-小計」欄）及資訊資產個別弱點與威脅之風險值（「風險值-小計」欄）。

5.7 撰寫風險評鑑報告

資訊安全工作小組依據風險評鑑結果撰寫「資訊-程序-06-03 風險評鑑報告」，並分析資訊資產安全需求，提出可接受之風險等級建議，提報資訊安全執行小組審查及決定可接受之風險等級。

5.8 決定可接受之風險等級

5.8.1 資訊安全執行小組應審查「資訊-程序-06-03 風險評鑑報告」，並針對所提出之風險等級建議，決定可接受之風險等級。

5.8.2 可接受風險等級之決定因素：

5.8.2.1 風險嚴重（衝擊）程度

5.8.2.2 風險處理急迫性

5.8.2.3 可分配之資源

5.8.3 為確保未遺漏需處理之資訊資產風險，除決定可接受風險等級外，對於無法接受之資訊資產項目，亦應擬訂風險處理計畫。

5.9 擬訂風險處理計畫

5.9.1 依風險評鑑結果及可接受風險等級之決議，由資訊安全工作小組針對需降低風險等級之資訊資產擬訂風險處理計畫，以期將風險降至可接受之程度。

5.9.2 風險處理計畫應依據「資訊-程序-06-02 風險處理計畫表」之格式撰寫。

5.9.3 風險處理計畫之風險處理措施，應根據 ISO27001 對各項資



訊安全之要求目標，擬訂適當之處理措施及相關執行資源之資訊。

5.9.4 風險處理計畫應提報資訊安全執行小組審查後執行。

5.10 執行風險處理計畫

應依據風險處理計畫之風險處理項目、所需資源、預訂完成日期等規劃，執行各項風險控制措施，並將執行進度紀錄於「資訊-程序-06-02 風險處理計畫表」之「風險處理進度」欄。

5.11 評估風險處理計畫執行成效

5.11.1 風險處理計畫於預訂完成日期結束後，須由資訊安全工作小組針對進行風險處理之資訊資產，依本說明書之風險評鑑程序實施風險重新評鑑，並紀錄於「資訊-程序-06-04 殘餘風險評鑑工作表」，以確認風險處理計畫之執行達到風險減緩預期效益之目標，並將風險重新評鑑之結果提報資訊安全執行小組。

5.11.2 若經風險重新評鑑後，資訊資產之風險值未達預期效益，亦即仍處於不可接受之風險等級，資訊安全工作小組則需依本程序書之風險處理程序進行風險再處理作業或接受該項風險。

6.附件

6.1 資訊-程序-04-01 資訊資產清冊

6.2 資訊-程序-06-01 風險評鑑工作表

6.3 資訊-程序-06-03 風險評鑑報告

6.4 資訊-程序-06-02 風險處理計畫表

6.5 資訊-程序-06-04 殘餘風險評鑑工作表。