環　球　科　技　大　學

資訊安全風險評鑑管理程序

文件編號：ISMS-02-006

機密等級：一般

版　　次：4.2

發行日期：2019/10/30

環球科技大學

文件名稱	資訊安全矯正管理程序	版本	4.1
文件編號	ISMS-02-004	發行日期	2019/10/30
		頁次	-

修　訂　紀　錄

版次	發行日期	修訂頁次	修訂者	修訂內容摘要
1.0	2010/08/01			新制定
2.0	2010/11/01	P.2,P.4		1. 5.2.1 修訂資訊資產價值 2. 5.4.3 將“高階主管”改為“圖資處主任”
3.0	2011/07/29	P.1,P.5		1. 因應本校內控文件之編號統一管理，以 ISMS 為文件範圍之識別。 2. 修改使用表單之文件編號。
3.1	2012/09/13	P.1		內文中本中心改為圖資處
		P.1		修正各項小組名稱
		P.4		修正風險評估作業報告對象
		P.5		增加風險評鑑報告撰寫之作業敘述
3.2	2013/07/31	P.1		1. 將個人資料納入資訊資產範圍 2. 修正驗證範圍
3.3	2015/04/30	P.1		刪除驗證範圍，統一列於適用性聲明書
3.4	2016/10/07	P.1,P.4,P.6-P.8		修訂單位名稱
4.0	2016/10/07	P.1-P.3		配合新版「教育體系資通安全暨個人資料」管理規範修訂

環球科技大學

文件名稱	資訊安全矯正管理程序	版本	4.1
文件編號	ISMS-02-004	發行日期	2019/10/30
		頁次	-

修　訂　紀　錄

版次	發行日期	修訂頁次	修訂者	修訂內容摘要
4.1	2016/11/23	P.6		配合新版「教育體系資通安全暨個人資料」管理規範補修訂參考文件
4.2	2019/10/30	P.1-P.2	巫正淵	資安/個資保護相關作業程序為因應資訊安全委員會及個人資料保護管理暨指導委員會合併為資訊安全暨個人資料保護管理委員會修正

環球科技大學

文件名稱	資訊安全矯正管理程序	版本	4.1
文件編號	ISMS-02-004	發行日期	2019/10/30
		頁次	-

目　錄

環球科技大學

文件名稱	資訊安全風險評鑑管理程序	版本	4.2
文件編號	ISMS-02-006	發行日期	2019/10/30
		頁次	1 / 10

1. 目的：

建立圖書資訊處資訊資產(含個人資料)風險評鑑之標準，以計算資訊資產價值、鑑別與分析風險來源、弱點與威脅所導致之資訊安全風險，並依據風險評鑑結果採取對策或控制措施，以降低資訊資產遭受損害的風險。

2. 範圍：

本校圖書資訊處所屬有關資訊機房之硬體/軟體、資訊、人員、基礎設施與服務。

3. 權責：

3.1 資訊安全暨個人資料保護管理委員會

3.1.1 依據風險評估結果，決定可接受風險等級。

3.1.2 審查風險處理執行成效。

3.1.3 決定風險評鑑時機與範圍。

3.1.4 維護系統化之風險評鑑方法。

3.1.5 監督風險評鑑之執行。

3.2 資訊安全組

3.2.1 管理與維護資訊資產清冊。

3.2.2 確認資訊資產清冊中群組化的方法以及認定進入風險評鑑的項目

3.2.3 執行風險評鑑作業，產出「資訊資產風險評估表」。

3.2.4 擬訂「風險處置計畫」並執行。

3.2.5「殘餘風險表」的產出，確保高階主管認同殘餘風險的結果

4. 名詞解釋：

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)：資訊資產面臨的事件，可能會對系統或組織及資產造成傷害，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乘，而造成資產損害的狀況。資產的弱點本身並不會造成傷害。

4.4 風險管理(Risk management)：管理和控制組織風險的協調活動。

4.5 風險評估(Risk evaluation)：對資訊資產所可能產生的威脅及弱點進行評估，並依據發生的衝擊與頻率來評估風險的等級。

4.6 風險處理(Risk treatment)：為改變風險，選擇與實施有效控制之過程。

4.7 風險擁有者(Risk Owner)

4.7.1 組織內針對各項資訊資產風險管理具備核准與確認者。

4.7.2 本校風險擁有者為各系統使用單位負責人。

4.8 資產價值：(資產評價 C、I、A)

4.8.1 機密性(Confidentiality)：資訊不可用或不揭露給未經授權之個人、個體或過程的性質。

4.8.2 完整性(Integrity)：防護資產正確性與完整性的特性。

4.7.3 可用性(Availability)：在授權核可要求下，得以存取及使用之特性。

5. 內容：

5.1 風險評鑑時機與對象：風險評鑑作業應每年定期執行，由資訊安全暨個人資料保護管理委員會決定執行時機與範圍。先以「資訊資產風險評估表」，針對所負責的資訊資產執行威脅性影響評估，並以五分量表的模式來表現其發生之資訊資產受到風險影響資產受損之嚴重度。

5.1.1 風險評鑑對象

5.1.1.1 資訊資產價值總數值(C+I+A)若為 11（含 11）以上，必須執行風險評鑑與處理措施。

5.1.1.2 資訊資產之機密性、可用性及完整性之數值，若其中一項數值為 5 者，必須執行風險評鑑與處理措施。

5.1.1.3 依據「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，其安全等級屬最高等級者，應執行風險評鑑與處理措施。

5.1.1.4 屬核心業務資訊系統者，應執行風險評鑑與處理措施。

5.1.2 鑑別風險來源與分析

5.1.2.1 應參考 ISO 31000，根據內外部議題鑑別風險來源，並參考 ISO 27005 分析評估內、外部環境因素與相關利害團體之資安風險，將各類資訊資產可能面臨之威脅與弱點項目，分別建立「資訊資產風險評估表」。其風險來源類別鑑別如下：

5.1.2.1.1 管理活動及控制不足

5.1.2.1.2 人員資安意識、教育訓練不足

5.1.2.1.3 實體環境控管不安全

5.1.2.1.4 軟硬體過時或缺乏軟硬體維護

5.1.2.1.5 系統漏洞或應用軟體開發不安全

5.1.2.1.6 安全防禦系統無效

5.1.2.1.7 網通架構方式不安全

5.1.2.1.8 駭客入侵

5.1.2.1.9 商譽、財務與法律關係

5.1.2.1.10 天災等不可抗力因素

5.2 風險評鑑方法：風險評鑑為計算資訊資產風險值之程序，用以決定風險處理優先順序。而「資訊資產價值」是以機密性、完整性、可用性三項因子所構成。再考量「資訊資產價值」分析其風險來源，針對可能面臨或已發生的資訊安全弱點與威脅發生的衝擊性與可能性進行評值。

5.2.1 資訊資產價值：資訊資產價值乃依資訊資產之機密性、完整性及可用性進行規劃及進行相關風險評鑑作業。

機密性：見附件一。

完整性：見附件二。

可用性：見附件三。

威脅標準定義如下：

評估標準	數值	發生頻率	備註
極高	5	每週發生一次以上	5 分為不可接受
高	4	每月發生一次以上	
中	3	每季發生一次以上	
低	2	每年發生一次以上	
極低	1	很少發生	

5.2.3 弱點標準定義如下：

評估標準	數值	發生頻率	備註
極高	5	每月發生一次以上	5 分為不可接受
高	4	每季發生一次以上	
中	3	每學期發生一次以上	
低	2	每年發生一次以上	
極低	1	很少發生	

5.2.4 衝擊標準定義如下：

影響營運(包含暫停)天數	數值	備註
72 小時以上	5	
24 小時以上～72 小時(含)	4	4 分為不可接受
8 小時以上～24 小時(含)	3	
4 小時以上～8 小時(含)	2	
4 小時(含)以下	1	

5.2.5 風險值計算：

5.2.5.1 資訊資產價值 = 機密性（C）、 完整性（I）、可用性（A）

【取三者最大者做為資產價值的代表】

5.2.5.2 風險值 = 資訊資產價值 ╳威脅╳弱點╳衝擊

5.3 風險評估完成後，應由執行風險評鑑人員對應「資訊資產風險評估表」中的高風險值項目，提出風險回應計畫，經單位主管審核後執行。

5.4 風險回應計畫處理原則：

5.4.1 資產價值、威脅、弱點、衝擊：資訊安全組每年至少應重新審查重要度、威脅、弱點、衝擊之處理基準值，考量原則為組織對資訊資產本年度之依賴狀態。

5.4.2 風險優先值處理基準值設定：資訊安全組每年依風險評鑑結果進行風險優先值之計算與處理基準設定。

5.4.3 向執行秘書報告風險評估結果：資訊安全組依據風險評鑑結果對執行秘書分析各組資訊資產安全需求，提出可接受之風險等級建議，由執行秘書決定可接受風險等級。

5.4.4 決定風險等級後，資訊安全組應將不可接受風險等級之資訊資產彙整到「風險處置計畫表」進行風險回應方式的確認。

5.5 風險處置

5.5.1 可接受風險等級之修訂：由執行秘書依圖書資訊處資訊安全環境、風險嚴重程度、風險處理的急迫性或可分配資源的有限性來制定/修訂接受風險之等級，必要時，可在「資訊資產風險評估表」以及「風險處置計畫表」中定義。

5.5.2 擬訂風險處理方式：依風險評鑑結果及可接受風險等級之決議，由資訊安全組針對需降低風險等級之資訊資產擬訂風險處理改善計畫，以期將風險降至可接受程度。

5.5.3 執行「風險處置計畫」：應依據風險處理資訊資產項目、所需資源、預訂完成日期等規劃，執行各項風險改善控制措施，並進行紀錄。

5.5.4 評估風險處理執行成效

5.5.4.1 風險處置計畫於預定完成日結束後，由資訊安全組針對風險處理計畫項目，

依本文件的風險評鑑流程重新實施風險評鑑，以確認風險處置方案的結果是否已達到可接受風險之程度。

5.5.4.2 經重新風險評鑑後，資訊安全組依風險評鑑結果撰寫「風險評鑑報告」，資訊資產風險值未能達到可接受風險的範圍時，應由資訊安全組認定殘餘風險，將該資訊資產項目轉至「殘餘風險表」，送交執行秘書審查。

6. 參考文件：

6.1 教育體系資通安全暨個人資料管理規範

6.2 ISO 27001:2013

6.3 附件一：資訊資產機密性評估基準

6.4 附件二：資訊資產完整性評估基準

6.5 附件三：資訊資產可用性評估基準

7. 使用表單：

7.1資訊資產風險評估表(ISMS-04-016)

7.2風險處置計畫表(ISMS-04-017)

7.3殘餘風險表(ISMS-04-018)

附件一：資訊資產機密性評估基準

量化值	機密性			
	人員	資訊	硬、軟體	基礎設施/服務
5	人員所接觸的資料足以影響全圖書資訊處。	當該資產機密性被破壞時，會造成本圖書資訊處業務目標完全無法達成或是圖書資訊處的聲譽受到重大負面衝擊。	一旦硬、軟體遭受技術性的侵入或破壞，使機密性無法維持，必須重新進行購置、複製成本極高，或屬移動性、風險極高之設備與媒體，對圖書資訊處全體同仁的工作與業務目標會產生極重大影響。	基礎設施涵蓋整體解決方案與硬體、軟體的結合性非常高，或影響全圖書資訊處。
4	人員所接觸的資料僅影響圖書資訊處內多餘一個組別以上。	當該資產機密性被破壞時，會造成本圖書資訊處 3/4 業務目標將無法在原訂目標時程完成。		基礎設施涵蓋整體解決方案與硬體、軟體的結合性高，或影響圖書資訊處 3/4 區域。
3	人員所接觸的資料僅影響圖書資訊處內的特定的系統。	當該資產機密性被嚴重干擾時，會造成本圖書資訊處 1/2 的業務目標無法在原訂目標時程完成。		基礎設施的設計與方案與硬體、軟體各自獨立考慮；或影響圖書資訊處 1/2 區域。
2	人員所接觸的資料影響圖書資訊處內的單一系統。	當該資產機密性被干擾時，會造成資訊室本身的業務目標無法完成，並且本圖書資訊處 1/3 的業務目標無法在原訂目標時程完成。	一旦硬、軟體遭受技術性的侵入或破壞，使機密性無法維持，必須重新進行調整、複製成本較低，或屬移動性、風險性一般之設備與媒	基礎設施涵蓋整體解決方案與硬體、軟體的結合較為不足；或影響圖書資訊處 1/3 區域。

量化值	機密性			
	人員	資訊	硬、軟體	基礎設施/服務
1	人員所接觸的資料都是普遍傳達的資訊。	當該資產機密性被干擾時，會造成圖書資訊處本身的業務目標部份無法完成，但是對於本圖書資訊處的整體業務目標的達成不構成影響。	體，對圖書資訊處單一部門或同仁之工作與業務目標產生影響較小，但還是能達成目標。	基礎設施涵蓋整體解決方案與硬體、軟體的完全無關，必須要靠重新改造基礎設施才能夠加入新的硬體設施架構；或僅影響機房。

附件二：資訊資產完整性評估基準

量化值	完整性			
	人員	資訊	硬、軟體	基礎設施/服務
5	被指定的人員完全熟悉指定的工作／流程系統並且有充分教導其他人員的能力。	流程輸出的結果完全不符合使用期望；或保存不當造成全部毀損、被破壞、遺失。	系統完整性受到破壞時，全圖書資訊處的終端使用者將無法順利的運用系統達成業務目標。	維持硬體、軟體的基礎設施/服務能夠依照原訂的機能正常的運作。
4	被指定的人員完全熟悉指定的工作／流程並且有教導其他人員的能力。	流程輸出的結果不符合使用期望，必須透過大量的輔助工具或是目視比對找出需求期望的資料；或保存不當造成 3/4 毀損、被破壞、遺失。	系統的完整性受到破壞時，有大部分的圖書資訊處內單位會受到該系統的影響無法正常運作，達成業務目標。	維持硬體、軟體的基礎設施/服務能夠正常運作，但是功能略有缺陷。
3	被指定的人員完全熟悉指定的工作／流程。	流程輸出的結果不符合使用期望，透過局部的輔助工具或是公式比對找出需求期望的資料；或保存不當造成 1/2 毀	系統的完整性受到破壞時，有大部分的圖書資訊處內單位感到系統效率略有低落，少數終端使用者已經開始反應系	維持硬體、軟體的基礎設施/服務能夠運作，但是如果在指定時間不能夠恢復機能將很快的影響硬體、軟體正常運行。

量化值	完整性			
	人員	資訊	硬、軟體	基礎設施/服務
		損、被破壞、遺失。	統有缺陷，終端使用者預定檔案或是功能運作緩慢。	
2	被指定的人員完全了解指定的工作／流程，但是緊急時還需要熟練的同仁支持才能完成工作。	流程輸出的結果，局部不符合使用期望，藉由經過訓練的人員重複的比對找出期望的資料；或保存不當造成 1/3 毀損、被破壞、遺失。	系統的完整性受到破壞時，只有部分圖書資訊處內單位使用該系統的同仁受到影響，系統反應不敏銳，但是終端使用者沒有明顯的感覺。	維持硬體、軟體的基礎設施/服務不能運作，系統的運行已經受到影響。
1	被指定的人員能夠操作指定的工作／流程。	流程輸出的結果，少數不符合使用期望，藉由使用者自行調整即可找出期望的資料；或保存不當造成 1/4 毀損、被破壞、遺失。	系統硬體、軟體、作業系統與資料庫均能夠依照原訂規格預期要求的作業。	維持硬體、軟體的基礎設施/服務不能運作，系統崩潰不能夠迅速解決。

附件三：資訊資產可用性評估基準

量化值	可用性			
	人員	資訊	基礎設施/服務	硬、軟體
5	執行工作的負責人員出勤時數及有效執行工作時間應達到該職務的 90%以上。	指定的流程、產出的結果及代理人員每日需要關注超過 2 次以上，警報系統（自動知會管理者）通知時，必須要視為最優先的處理項目。		該項資產應用頻率以 24 小時不間斷。
4	執行工作的負責人員出勤時數及有效執行工作時間應達到該職務的 80%以上。	指定的流程、產出的結果及代理人員每日需要關注超過 1 次以上，警報系統（自動知會管理者）通知時，必須要視為優先的處理項目。		該項資產應用頻率以周計。
3	執行工作的負責人員出勤時數及有效執行工作時間應達到該職務的 70%以上。	指定的流程、產出的結果及代理人員每週需要關注超過 2-4 次以上，警報系統（自動知會管理者）通知時，必須要視為一般的處理項目。		該項資產應用頻率以月計。
2	執行工作的負責人員出勤時數及有效執行工作時間應達到該職務的 60%以上。	指定的流程、產出的結果及代理人員每月需要關注超過 2 次以上。		該項資產應用頻率以季度衡量。
1	執行工作的負責人員出勤時數及有效執行工作時間應達到該職務的 50%以上。	指定的流程、產出的結果及代理人員每月需要關注超過 1 次以上，		該項資產應用視流程需求啟動。