雲林縣西螺鎮公所

風險評鑑與管理程序

文件編號： XLTG-02-005

版　　次： V1.0

文件日期： 110 年 11 月 24 日

機密等級： 普通

文件制/修訂履歷

制/修訂 版次	制/修訂 日期	制/修訂 說明	作 者	備 註
V1.0	110.11.24	初版發行	ISMS 執行小組	

目　　錄

壹、 目的

雲林縣西螺鎮公所(以下簡稱本所)為維護資訊業務營運安全，就重要資產識別其可能面臨的風險可能性與可能的後果，決定其可接受風險等級與處理優先順序，並施予適當之控制措施，以有效管控風險，降低資訊安全事故的發生機率與影響程度，特訂定本「風險評鑑與管理程序」(以下簡稱本程序)。

貳、 適用範圍

本程序適用於本所資訊業務風險評鑑與風險管理相關事宜。

參、 權責

一、 資安長或其授權人核定、發布本程序。

二、 資訊安全管理委員會

（一）核定風險評鑑結果。

（二）決定可接受風險等級。

（三）核定適用性聲明。

三、 ISMS 執行組組長審查本程序，並督導本程序之執行。

四、 ISMS 執行小組

（一）研擬、評估及檢討本程序。

（二）執行風險評鑑。

（三）研提可接受風險等級建議。

（四）執行風險管理。

（五）研擬風險處理及應變計畫，並提出風險再評鑑需求。

（六）風險發生時，執行緊急應變措施。

五、 ISMS 承辦人

（一）協調及彙總本程序之進行。

（二）彙整所有控制措施，製作適用性聲明文件。

肆、 定義

一、 機密性（Confidentiality, C）：使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(確保只有獲得授權的人員及程式才能存取資訊)。

二、 完整性（Integrity, I）：保護資產的準確度(accuracy)和完全性(completeness)的性質(確保資訊與處理方式精確性及完整性)。

三、 可用性（Availability, A）：經授權個體因應需求之可存取及可使用的性質(確保獲得授權的使用者在需要時可以使用)。

四、 法規或合約遵循性（Legal, L）：符合法律、法規及契約要求的性質。

五、 威脅（threats）：可能導致資產遭受傷害之潛在原因。

六、 脆弱性（vulnerability）：能被威脅利用之資產自身之弱點或漏洞(資產自身之弱點或漏洞，將促使威脅利用此弱點而造成資產傷害)。

七、 風險值（risk）：指資產遭受威脅造成風險之可能性高低。

八、 剩餘風險（residual risk）：執行了迴避、轉移、減緩等風險管理工作，或實施風險處理相關措施後仍殘留、存在的風險。

九、 風險分析（risk analysis）：系統性的使用資訊，以辨識風險及估計風險。

十、 風險評鑑（risk assessment）：風險分析與風險評估的整個過程。

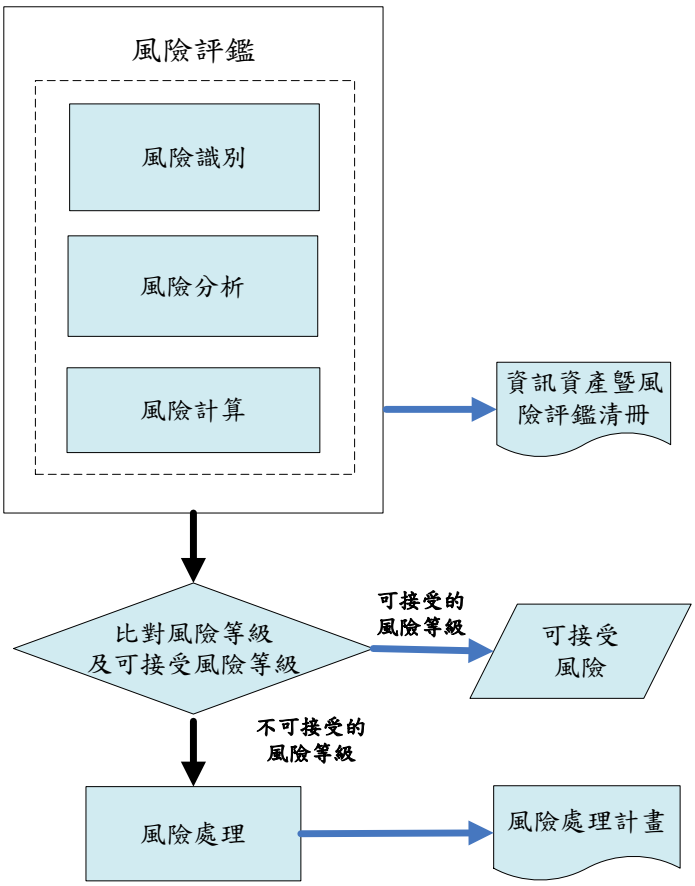
十一、風險處理（risk treatment）：選擇與實施控制措施的過程，藉以修正風險。

十二、可能性: 風險發生的可能性。

十三、可能的後果: 風險發生後可能造成的後果。

伍、 管理項目

風險評鑑作業係依據本所「資訊安全手冊」所界訂之 ISMS 範圍，對營運有影響性的資產評估其價值及法規或合約遵循性，識別出該資產可能面臨的威脅與弱點，於計算其風險值後，就超過可接受風險等級的資產排定優先處理順序，進行風險處理。風險評鑑與管理之作業流程，如下圖。



一、 風險評鑑作業方式

（一）風險識別

ISMS 執行小組應與資訊安全管理系統內相關業務人員溝通及諮詢，必要時得召開會議，以共同討論形式，儘可能識別出對本所造成影響的潛在風險，並考慮依現有控制措施，將風險來源與其描述記錄於「風險評鑑清冊」。

（二）風險分析

風險識別完成後，ISMS 執行小組應分析各項風險發生之可能性及發生後造成的影響程度，若已有控制措施，應將現有控制措施完整度納入分析。評估準則如下。

1. 現有控制措施完整度

控制措施完整度評估標準	等級	控制措施評等	範例參考
控制措施非常完善	完整	1	對於風險已施行管理規範與技術軟、硬體進行管理。
僅有部份控制措施	可改善	2	已有部份管理規範或其它技術性管控（例如:軟、硬體佈署、人工定期檢督控制紀錄)。
不足控制措施	不足	3	無實行管理規範，亦無技術軟、硬體管理。

2. 風險發生可能性評估準則

可能性評估標準（滿足其中一項即可）	等級	可能性評等
不可能發生或從未發生（50%以下)。 每季可能發生 1 次。	不太可能	1
有可能發生（50%)。 每季可能發生 2 次～5 次 （若未有自動化或人為監控風險機制，至少應評到此等級)。	時常	2
發生機率非常高或很有可能發生（50%以上)。 每季可能發生 5 次以上。	非常可能	3

（三）風險影響程度評估準測

判斷發生該風險時，對於本所資產的影響程度（損失、損害程度)，可由機密性（Confidentiality)、完整性（Integrity)、可用性（Availability）及法規遵循性（Compliance）四方面綜合考量，亦可視組織關鍵業務屬性給予衝擊評等進行權重調整。

公式：風險值=

（機密性衝擊+完整性衝擊+可用性衝擊+法規遵循性衝擊）x 控制措施評等 x 可能性評等

（四）訂定風險等級

風險等級最高的至最低分別以 A、B、C、D 代表

風險等級	說明
A	屬於高風險值，且風險發生可能性高，控制措施不足或僅有部份，以會議討論方式決定是否緊急處理。
B	屬於中風險值，且風險發生可能性高，控制措施不足或僅有部份，以會議討論方式決定是否緊急處理。
C	屬於中風險值，且風險發生可能性低且控制措施完善，非急迫性之風險，以會議討論方式決定是否緊急處理。
D	屬於中低風險值，且風險發生可能性低且控制措施完善，非急迫性之輕微風險，可接受此類風險。

將各風險分析項目值、風險等級填寫於「資訊資產暨風險評鑑清冊」。

（五）訂定可接受風險等級

當風險等級產出後，ISMS 執行小組以會議方式應就該次風險分析結果決定一適當之可接受風險等級，記錄於「風險評鑑清冊」，並與所有風險之風險等級比較。當風險等級大於可接受風險等級時，應由 ISMS 執行小組協調並指定風險負責人。

（六）風險處理

1. 風險負責人應指定人員評估處理高風險等級之方式，並決定對應之控制措施，提交 ISMS 執行小組填寫於「風險處理計畫表」
2. 風險處理可採取以下措施：降低風險、接受風險、迴避風險或轉嫁風險。
3. 各項風險處理方式應由風險負責人核准。
4. 針對高風險的項目，於風險處理預定完成日前施以控制措施後，須由風險負責人監督其控制措施是否有效，可採用風險再評鑑或其它量測方式，並將其風險處理狀態於管理審查會議中進行確

認。

二、 風險評鑑之時機

風險評鑑每年執行1次，不定期的執行方式則可考慮如下狀況：

（一）重大設備、所使用之資訊處理技術或系統架構變更。

（二）任何有關本所業務異動或營運流程的改變足以影響資訊安全。

（三）發生重大異常事件或資安事故。

（四）其他外部事件，諸如法律或法規環境之變化、已變更之契約義務及社會氛圍之變化等。

陸、 參考文件

一、 ISO27001/CNS27001。

二、 ISO27002/CNS27002。

三、 資產分類與管理程序。

四、 資訊安全組織管理程序。

柒、 使用表單

一、 風險評鑑表

二、 風險處理計畫表