雲林縣西螺鎮公所

資訊安全稽核程序

文件編號： XLTG-02-002

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)為確保資訊安全管理系統(以下簡稱 ISMS)相關程序能有效落實，運作過程中所發生的異常事件、不符合事項及需改善事項得以適當處理，並達成持續改善的目標，特訂定本「資訊安全稽核程序」(以下簡稱本程序)。

貳、 適用範圍

本程序適用於本所資訊安全管理系統相關控管流程的稽核事宜。

參、 權責

一、 資安長或其授權人核定、發布本程序。

二、 ISMS 稽核小組組長審查本程序，並督導本程序之執行。

三、 ISMS 稽核小組研擬、評估及檢討本程序。

四、 ISMS 承辦人協調及彙總本程序之執行。

五、 本所政風室負責資訊安全管理系統內部稽核幕僚作業。

六、 受稽核單位

（一）依稽核計畫接受稽核、安排場所、工作人員，並準備相關作業資料。

（二）參加稽核啟始會議及結束會議。

（三）依據稽核結果，規劃並執行適當的矯正措施。

肆、 定義

一、 稽核發現:依據「內部稽核檢核表」,經實地調查後所查得之事實。

二、 評核原則：說明如下表。

評核結果	評　核　說　明
符合	1.實際作業依照書面規範進行。 2.紀錄及簽核作業皆按照規定辦理。
觀察事項 (潛在不符合)	1.已建立書面規範，但尚未有實際作業需求。 2.尚未發生或未達時間點，尚不能判定符合或不符合之事項。 3.經觀察實際執行情形，研判繼續發展有可能無法達到標準或程序規範要求者。
次要不符合	1.人員雖按照規範執行作業，但於過程中發生疏失。 2.未能完全遵循一項或多項 ISMS 之要求，但為單一事件者。 3.人員作業達到安全控制之目的，但尚未建立完整書面程序或紀錄。
主要不符合	1.尚未規劃或執行相關安全管理規定。 2.違反自訂之管理規範。 3.違反 ISO27001 或 CNS27001 標準之要求。 4.未能執行一項或多項 ISMS 之要求，或同一輕微不符合事項多次發生。
不適用	稽核範圍內作業無需使用的控制項目

三、 稽核人員之資格：

稽核人員應具備下列條件之一：

（一） 本所政風室相關工作之人員(需受過內部稽核訓練)。

（二） 曾參加內部稽核相關訓練課程之人員。

（三） 領有電腦稽核或資訊安全稽核相關證照之人員。

四、 矯正措施：為消除已經發生的不符合及潛在可能發生的不符合事項所採取的措施。

五、 持續改善：採取矯正措施，使本所之 ISMS 能依循規劃、執行、檢查與矯正的模式持續改進。

伍、 管理項目

ISMS 稽核小組應規劃每年至少執行一次 ISMS 內部稽核作業，並由本所政風室負責相關之幕僚作業。

實施內部稽核得調閱受稽核單位相關資料、實地測試或檢查資訊安全相關之軟、硬體設備使用情形，並請相關作業人員提供說明及補充相關書面資料。內部稽核流程請參見下頁圖 5-1 所示，相關作業說明如下：

一、 規劃內部稽核作業期程

（一）內部稽核每年應至少執行一次，ISMS 稽核小組並可視情況實施不定期之稽核。

（二）ISMS 稽核小組於每年年底前，規劃下一年度之稽核工作，稽核範圍應涵蓋實施 ISMS 之各相關單位，並包括 ISMS 之所有流程。

（三）規劃內容應包含以下項目：

1. 本所資訊安全改善項目、目標、實施及監控方式。

2. 稽核作業組織及權責。

3. 內部稽核作業時程及報告方式。

4. 內部稽核作業人力及資源需求。

5. 資料管理機制。

（四）稽核規劃結果須經 ISMS 稽核小組組長審查，並陳報資訊安全管理委員會召集人同意後實施，修正時亦同。

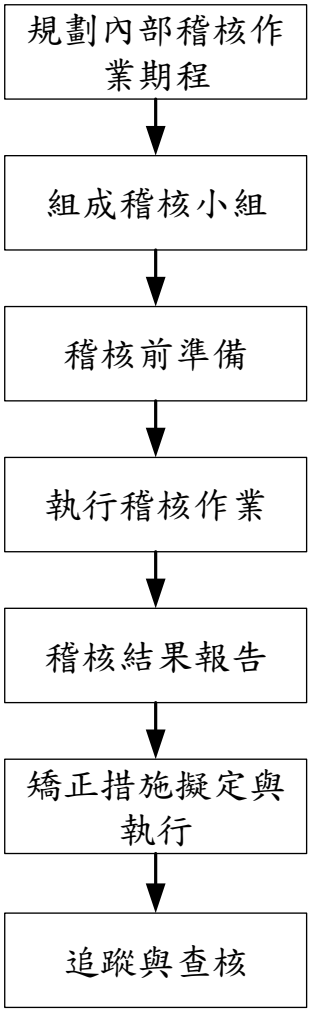

圖 5-1：內部稽核與矯正流程圖

二、 組成稽核小組

ISMS 稽核小組應於稽核執行前，協調成立內部稽核小組，成員包含稽核小組組長與稽核員。內部稽核小組人員須曾接受稽核相關教育訓練，且不可稽核自己所負責之業務，ISMS 稽核小組可視需要，安排稽核員之訓練課程。

（一）稽核小組組長

稽核小組組長應由資深且具備稽核經驗之合格稽核員擔任，其權責為：

1. 擬定內部稽核計畫，並取得資安長同意。
2. 召開內部稽核啟始及結束會議。
3. 擬定內部稽核檢核表。
4. 主導內部稽核作業。
5. 撰寫內部稽核報告。
6. 確認稽核小組所開立之「資訊安全矯正措施處理表」均已完成矯正或處理完畢。

（二）稽核員

內部稽核小組成員可由各單位推薦適當人員作為候選稽核員，稽核組長應考量稽核工作需求、人員特質、經驗及訓練等因素，自候選稽核員中選擇適當人員擔任稽核員。其權責為：

1. 協助稽核小組組長擬定內部稽核檢核表。
2. 協助進行內部稽核作業。
3. 記錄稽核發現。
4. 撰寫稽核發現於「資訊安全矯正措施處理表」。
5. 複查與追蹤稽核所發現不符合事項之改善措施。
6. 確認所開立之「資訊安全矯正措施處理表」已完成矯正或處理完畢。

三、 稽核前準備

內部稽核小組應於稽核前辦理下列準備工作：

（一）稽核小組組長帶領內部稽核小組成員，依據本所流程實施狀況及資訊安全防護之改善需求，研讀與被稽核單位有關之 ISMS 文件及稽核歷史紀錄等，設定稽核目標及範圍，製作成「內部稽核檢核表」，並確認該單位之待查核事項以及稽核工作涵蓋度是否足夠。

（二）稽核小組組長依據「內部稽核檢核表」之待查核事項，規劃稽核時程與任務編組，擬定「內部稽核計畫」。

（三）稽核小組組長應將準備完成之「內部稽核檢核表」及「內部稽核計畫」，至少於表訂稽核日兩週前移請 ISMS 稽核小組簽奉資安長同意實施後，發文通知受稽核單位，受稽核單位如有疑義，應儘速提出與內部稽核小組再行確認。

（四）稽核小組組長應召開內部稽核前稽核小組會議，向全體稽核員說明該次稽核之時程、範圍、分工、及須注意事項等，以取得稽核共識。

四、 執行稽核作業

內部稽核小組應依事先規劃之日期與時程執行稽核作業，並將結果回報給 ISMS 稽核小組。

（一）啟始會議

1. 由稽核小組組長召開啟始會議，向受稽核單位說明本次稽核之時程、範圍、配合事項及須注意事項，並對稽核計畫安排等與相關人員協調確認後，宣布稽核開始。
2. 參與啟始會議之人員原則如下：
   (1)內部稽核小組全體組員。
   (2)受稽核單位主管及主要人員。
   (3)ISMS 執行小組成員。
3. 稽核啟始會議應留有簽到紀錄以供備查。

（二）執行稽核

1. 內部稽核小組應依「內部稽核檢核表」所列項目，對受稽核單位之實際作業狀況進行查核，並將所見事實記錄於「內部稽核檢核表」。
2. 內部稽核應秉持客觀、公正無私的態度進行，受稽核部門應配合稽核工作。
3. 稽核時若發現不符合事項，應將事實記錄於「資訊安全矯正措施處理表」。
4. 內部稽核結果的存取行為應作監控並留有紀錄。

（三）稽核員會議

1. 稽核結束後，稽核小組組長應召開稽核員會議，根據實地訪談、查閱紀錄、觀察、提問及實際測試所蒐集之客觀證據作出結論。
2. 稽核過程中若發現作業異常或未符合安全政策、法規及標準時，應詳實記錄並在稽核員會議內討論，以取得稽核團隊共同認可，經稽核組長確認後予以記錄。
3. 稽核組長或其指派人員，彙總各稽核員之稽核發現製作成簡報資料，於結束會議時向受稽人員說明稽核結果。

（四）結束會議

稽核結束時應舉行稽核結束會議，由稽核組長對受稽核單位報告稽核結果及發現事實，受稽核單位如有異議或補充資料，可於會議中提出並進行討論，稽核組長將結論記載於內部稽核報告中。

1. 參與結束會議之人員同啟始會議之人員。
2. 受稽核單位主管應瞭解並確認「資訊安全矯正措施處理表」內所記載之不符合事項，並簽名認可。
3. 受稽核單位主管應保留「資訊安全矯正措施處理表」正本，以作為擬定矯正措施時之依據。稽核組長應影印 1 份「資訊安全矯正措施處理表」攜回，以利執行後續作業。
4. 若受稽核單位與內部稽核小組對稽核結果有所爭議，且無法達成共識時，稽核組長可記錄爭議事項，轉請資訊安全管理委員會召集人協調仲裁，以達成共識。
5. 稽核組長應彙整稽核相關文件(包括「稽核通知」、「稽核計畫」、

「內部稽核檢核表」、「簽到表」、「資訊安全矯正措施處理表」等)，製作成為「稽核結果報告」，並交予 ISMS 稽核小組保管，以作為後續缺失矯正結果追蹤與複查之依據。

五、 稽核結果報告

(一) 稽核組長應彙整稽核執行狀況、「資訊安全矯正措施處理表」之件數與建議改善事項、分析稽核缺失之趨勢等，製作「稽核結果報告」。

(二) 「稽核結果報告」內容至少包括：稽核依據、稽核目的、稽核時間、稽核項目和範圍、稽核方法與稽核結論等。

(三) 「稽核結果報告」由 ISMS 稽核小組提報資安長，經資安長同意報告內容後，由 ISMS 稽核小組函發各相關單位。

(四) 不符合事項的矯正和追蹤

受稽核單位依據「稽核結果報告」及「資訊安全矯正措施處理表」，按「矯正措施處理程序」之規定進行矯正作業。

陸、 參考文件

一、 矯正措施處理程序。

二、 資訊安全組織管理程序。

三、 文件與紀錄管理程序。

柒、 使用表單

一、 資訊安全管理系統年度內部稽核計畫。

二、 資訊安全矯正措施處理表。

三、 資訊安全管理系統內部稽核結果報告。