中央研究院

資訊科學研究所

資訊安全稽核管理與矯正作業說明書

機密等級：□公開 ■內部 □敏感

編　　號：B330-I316

版　　本：1.0

核准日期：115 年 4 月 24 日

文件制／修訂紀錄表

版次	修訂日期	修訂單位	修訂者	核准者	修訂內容
1.0					新擬訂文件

目　錄

壹、目的

中央研究院資訊科學研究所（以下簡稱本所）為規範資訊安全管理系統稽核（以下簡稱資安稽核）之執行方式，以驗證本所資訊安全相關活動執行是否遵循資訊安全管理系統(ISMS)之要求，為運作過程中發生之缺失及潛在之風險，採取相關矯正及持續改善，以防止類似事件發生，進而訂定「資訊安全稽核與矯正作業說明書」(以下簡稱本說明書)。

貳、依據

一、資通安全管理法及其子法

二、中央研究院資通安全暨個人資料保護政策及規範

三、中央研究院資通安全管理規範實施要點

四、ISO/IEC 27001 資訊安全管理系統（Information Security Management System，ISMS）

參、範圍

本所資訊安全管理系統(ISMS)相關活動，均屬本說明書之適用範圍。

肆、權責

一、本所資安長

(一) 指派資訊安全稽核小組組長及成員。

(二) 審議及核定資通安全稽核計畫。

二、資通安全管理委員會

(三) 召開管理審查會議

(四) 審查 ISMS 稽核結果，以及各項矯正措施之執行狀況。

三、資訊安全稽核小組

(一) 擬訂資通安全稽核計畫。

(二) 稽核資訊安全管理制度之落實與遵行情形。

(三) 撰寫資訊安全管理制度稽核報告及提出建議。

(四) 追蹤缺失事項之執行情形並加以記錄。

(五) 協調提供稽核所需資源。

(六) 彙總稽核結果，提報管理審查會議。

四、 稽核小組組長

召集資訊安全管理稽核作業相關會議，並督導作業之執行。

五、 稽核小組成員

(一) 確保稽核業務依本程序書確實執行。

(二) 編製資通安全稽核檢核表。

(三) 報告稽核執行情形及成果。

(四) 列管「B330-I316-03 資通安全稽核報告」及所附相關查核資料。

(五) 配合稽核小組組長指示執行稽核作業完成各項紀錄及查證矯正

(六) 與預防措施執行情形。

(七) 稽核人員不得稽核自身負責之業務

六、 受稽核部門

(一) 應於稽核期間指派人員接受稽核，並協助調閱有關紀錄、報告或文件。

(二) 應就稽核所發現之缺失進行原因分析及影響評估，決定優先順序與處理時限提出矯正與預防措施並實施。

伍、作業說明

一、 稽核頻率

(一) 每年定期辦理 1 次資訊安全內部稽核作業。

(二) 視需要不定期執行專案稽核。

二、 稽核人員組成

稽核小組組長本所資安長指派專人擔任；小組成員 2 至 7 人由本所資安長遴選，協助小組組長執行資通安全稽核作業。為確保稽核過程之客觀性與獨立性，應由非受稽核人員擔任稽核人員。稽核人員資格要求如下：

(一) 稽核小組組長：須由具 ISO /IEC 27001 Lead Auditor 資格或受過相關稽核訓練者擔任。

(二) 稽核小組成員須由受過相關稽核訓練者擔任。

三、 稽核計畫擬定

為達稽核之有效性,稽核小組於稽核執行前應規劃並研擬「B330-I316-01 資通安全稽核計畫」, 做為執行稽核之指導綱要,其內容應包括:稽核範圍、稽核項目、稽核人員、稽核時程、稽核程序等,並須經本所資安長同意後實施,其修訂亦同。

四、 稽核準備

稽核小組於稽核前須協調完成下列事項:

(一) 確定稽核目標及範圍。

(二) 確定本次稽核組成員與分工。

(三) 稽核小組應遵循 ISO /IEC 27001 標準與本所於資訊安全管理系統之要求事項,研擬「B330-I316-02 資通安全稽核檢查表」,由稽核小組組長召開小組準備會議,提示稽核要點、協調分工及排定時程。

(四) 稽核小組應於查核前召開預備會議,並通知受稽核部門配合稽核事宜。

(五) 受稽核部門於接獲稽核通知後,應配合準備稽核所需相關資料。

五、 稽核執行

(一) 稽核小組組長應於稽核前召集資訊安全稽核小組、受稽核部門召開啟動會議,說明稽核範圍、時程、配合事項等。倘有需要,受稽核部門業務主管人員應就其執行狀況說明並確認稽核範圍。

(二) 稽核小組成員於稽核時應依抽樣原理收集足夠之客觀證據,以研判該稽核項目是否符合相關規範並有應保存之適當稽核存底。

(三) 稽核小組成員依「B330-I316-02 資通安全稽核檢查表」執行稽核,逐項填寫稽核結果 ,並對所獲悉之機密性或敏感性資料負保密責任。
「B330-I316-02 資通安全稽核檢查表」增修時, 須經稽核小組組長核定。

(四) 受稽核部門應尊重及支持稽核小組成員,誠實答覆稽核人員所提問題,並接受調閱有關紀錄、報告及文件。

(五) 為確保稽核過程的客觀性與獨立性,稽核人員之安排以不稽核所負責之工作或單位為原則,於稽核時抽樣收集之客觀證據,以研判稽核項目是否符合規範,並保存適當稽核軌跡與佐證資訊。

(六) 稽核人員於稽核時,應檢視本所人員遵守相關法令執行業務的符合性。

(七) 稽核時應對前次稽核發現不符合事項，及外部稽核發現之不符合事項進行追蹤。

六、 **稽核報告**

(一) 稽核實施之後，稽核人員應將稽核結果提交資訊安全稽核小組內部會議討論、彙整後由 稽核小組組長提出「B330-I316-03 資資通安全稽核報告」。

(二) 稽核小組組長應於稽核完成召開總結會議檢討稽核結果及發現，並 澄清疑義，稽核報告應請受稽核單位代表簽名。

七、 **矯正與預防措施**

(一) 受稽核部門於接獲稽核報告後，最晚於十個工作天內將該單位缺失之原因分析及擬採行之矯正與預防措施填列於「B330-I316-04 矯正處理單」內，並於受稽核部門主管核定後回覆資訊安全稽核小組。

(二) 為矯正 ISMS 於運作過程中實際發生之缺失，如遇有下列狀況應由缺失權責部門或發現人員填寫「B330-I316-04 矯正處理單」進行列管，就缺失或風險進行原因分析及影響評估，決定優先順序與處理時限並研擬缺失矯正措施，由缺失權責部門主管審查後執行。

1. 外部稽核發現不符合項目或缺失。
2. 發生資訊安全事故（含重大異常事故）或自行發現缺失。
3. 違反本所資訊安全政策之狀況。
4. 資訊安全目標一直無法達成。
5. 進行資訊安全日常管理及各種資料分析發現異常時。
6. 管理審查會議提出之改善事項。
7. 發生營運持續計畫中未考慮之重大災難事件。
8. 其他需矯正之狀況。

八、 **稽核結果彙總**

於稽核完成後，資訊安全稽核小組應彙整「B330-I316-02 資通安全稽核檢查表」及「B330-I316-04 矯正處理單」，以提報管理審查會議。

陸、參考文件

無

柒、使用表單

一、 B330-I316-01 資通安全稽核計畫

二、 B330-I316-02 資通安全稽核檢查表

三、 B330-I316-03 資通安全稽核報告

四、 B330-I316-04 矯正處理單