中央研究院

資訊科學研究所

管理審查及有效性量測作業說明書

機密等級：□公開 ■內部 □敏感

編　　號：B330-I318

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）為規範各項資訊安全管理制度之審查，以確保所建立之資訊安全管理系統得以有效運作，以及達成持續改善資訊安全管理系統、改善機會及符合資訊安全目標所衍生之績效標準，以維持其適用性、適切性和有效性，特訂定「管理審查及有效性量測作業說明書」（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、ISO/IEC 27001 資訊安全管理系統（Information Security Management System，ISMS）

參、範圍

本所各項資訊安全管理審查之實施，均適用本說明書。

肆、權責

一、本所資安長

(一) 管理審查會議決議事項之核定及其執行之督導。

(二) 審查並核定績效標準。

二、資通安全管理委員會

召集管理審查會議，審查資訊安全管理制度之實施情形。

三、資訊安全推動小組

(一) 製作管理審查會議資料，提供會議中討論。

(二) 會議紀錄之建立與維持。

(三) 會議記錄經資安長核定後，分送本所各部門留存及續辦。

(四) 跟催與複查本所各部門就資安長所核定管理審查會議決議事項之執行進度與情形。

(五) 依資訊安全目標、風險評鑑結果及改善機會擬定績效指標及達成方案。

(六) 定期實施量測與監督。

四、 本所各部門

依據資安長核定之管理審查會議決議事項，執行各項資訊安全工作，包括資訊安全管理制度之改進措施與行動、風險評鑑與風險處理計畫之更新以及資訊安全管理流程與控制措施之修正等。

伍、作業說明

一、 管理審查會議之召開

管理審查會議由資訊安全管理委員會召集人(資安長)召開，每年至少召開一次，以確保資訊安全管理系統的適用性和有效性。

二、 管理審查會議之參加人員

資訊安全管理委員會全體成員以及本所各部門相關人員。

三、 管理審查會議之內容

每次管理審查會議召開前，由資訊安全推動小組製作管理審查會議資料，提供會議中進行討論，其審查內容應包括如下項目：

(一) 過往管理審查之議案的處理狀態。

(二) 與資訊安全管理系統有關之內部及外部議題的變更。

(三) 資訊安全績效之回饋，包括下列之趨勢。

1. 不符合項目及矯正措施。
2. 監督及量測結果。
3. 稽核結果。
4. 資訊安全目標之達成。

(四) 關注方之回饋。

(五) 風險評鑑結果及風險處理計畫之狀態。

(六) 持續改善之機會。

四、 管理審查會議之紀錄

管理審查會議由資訊安全推動小組負責記錄，經資訊安全管理委員會召集人(資安長)核定後，分送給本所各部門留存及續辦，並應依「B330-I301 文件控管作業說明書」之相關規定進行紀錄控管。

管理審查會議紀錄應填寫於「B330-I318-01 管理審查會議紀錄」，內容

應包括如下事項：

(一) 持續改善機會有關之決策，包括但不限於下列項目。

1. 與資通安全管理法暨其子法相關之改善項目
2. 修訂組織全景評鑑程序書
3. 改善管理系統年度量測指標
4. 改善年度各項稽核作業
5. 改善資安認知訓練
6. 更新風險評鑑結果與風險處理計畫

(二) 任何對資訊安全管理系統變更之需要，包括但不限於下列項目。

1. ISMS 有效性之改進措施與行動
2. 影響資通安全程序與控制之必要時的修改，以回應可能衝擊 ISMS 之內部或外部事件，包括下列事項之變更：
   (1) 各項營運要求
   (2) 各項安全要求
   (3) 影響既有各項營運要求的營運過程
   (4) 法律或法規各項要求
   (5) 契約的各項義務
   (6) 風險等級及/或風險接受準則
3. 資源需求
4. 控制措施的有效性如何量測之改進

五、 決議事項之跟催

經資安長核定之會議決議事項列為下次資訊安全內部稽核作業之稽核要項，由資訊安全推動小組進行跟催與複查，以確保各項決議事項得以如期如質執行與改善。

六、 控制措施有效性的量測

資訊安全推動小組透過系統相關紀錄及資訊安全相關監控記錄與分析

報告中評估相關控制措施的量測紀錄，定期彙整、審查量測結果，並填寫「B330-I318-02 資訊安全目標有效性量測表」，確認達成預期的目標或修訂相關文件，俾利持續改善並強化整合性資訊安全管理，提高安全防禦強度。相關資訊彙整作為管理審查會議輸入的項目，針對有效性量測結果及改善措施做審查，以作為執行改善措施之依據。

陸、參考文件

B330-I301 文件控管作業說明書

柒、使用表單

一、 B330-I318-01 管理審查會議紀錄

二、 B330-I318-02 資訊安全目標有效性量測表