

中央研究院

資訊科學研究所

組織全景分析作業說明書

機密等級：公開 內部 敏感

編 號：B330-I303

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.....	4
貳、依據.....	4
參、適用範圍.....	4
肆、權責.....	4
伍、用語釋義.....	4
陸、作業說明.....	5
柒、參考文件.....	7
捌、使用表單.....	7

壹、目的

中央研究院資訊科學研究所（以下簡稱本所）透過分析組織全景樣貌，進而了解資通安全管理相關之內部及外部議題、關注方（Interested Party）對於資通安全的需求與期望，以決定資通安全管理統運作之範圍、資通安全政策、目標及風險改善機會。

貳、依據

- 一、中央研究院資通安全暨個人資料保護政策及規範
- 二、ISO/IEC 27001 資訊安全管理系統（Information Security Management System, ISMS）

參、適用範圍

本所資通全景分析事宜，均適用本作業說明書。

肆、權責

- 一、資通安全管理委員會
 - (一) 決定內部議題及外部議題。
 - (二) 決定資訊安全管理系統運作的範圍。
- 二、資安推動小組
 - (一) 檢視內部議題及外部議題。
 - (二) 提供內部議題及外部議題，供資通安全管理委員會參考。
 - (三) 瞭解關注方（Interested Party）對於資通安全的要求與期望，並彙總後供資通安全管理委員會參考。
 - (四) 彙整組織所執行的活動，與由其他組織執行活動期間的介面與相依性。
 - (五) 提出因應風險及機會的改善方式。

伍、用語釋義

- 一、組織：指資訊科學研究所
- 二、內部單位：指本所內部各單位
- 三、院內單位：指本所以外之中央研究院院本部、各所、中心及處。

四、外部單位：指中央研究院以外之單位

五、一般使用者：使用本所提供之資通服務者

六、關注方 (Interested Party)：對於資訊安全管理系統有所要求或期望之外部單位、院內單位、內部單位、及一般使用者。

陸、作業說明

一、組織全景分析作業

資安推動小組應參考組織架構或業務職掌每年至少一次或不定期（如組織異動或業務改變等）確認資訊安全管理系統之關注方，並將結果記錄於「組織全景評鑑表」中。

二、內部議題及外部議題分析與管理

資安推動小組應考量符合組織目的及資訊安全管理系統之成效，定期檢視下列內部議題及外部議題，將結果記錄於「組織全景評鑑表」中，並於管理審查會議上提出新增或修改之建議，以決定資訊安全管理系統範圍之依據。

(一) 內部議題

1. 組織治理、組織結構、角色和責任。
2. 政策和目標，及在不同的地方實現這些目標的策略。
3. 能力、理解資源和知識的條款（如資金、時間、人員、流程、系統和技術）。
4. 內部利益相關者、組織的文化、觀念和價值。
5. 資通系統、資訊流和正式或非正式的決策過程。
6. 相關標準及適用組織指導方針和模式。
7. 形式和契約關係的程度。

(二) 外部議題

1. 國際、國家、區域抑或地方，其社會與文化、政治、法令、規章、財務、技術、經濟、自然及競爭環境。
2. 對組織的目標具有衝擊之主要推動者與趨勢。
3. 與外部利害關係者的關係，以及外部利害相關者之價值。

三、瞭解關注方之需要及期望

資安推動小組應依據「組織全景評鑑表」中的外部單位、院內單位、內部單位等關注方，透過訪談、公開網站或內部網站、電子信箱等方式找出關注方之要求（包括法律、契約等）及期望，將其彙總後提供給資通安全管理委員會參考，以作為決定資訊安全管理系統範圍之依據。

四、活動間的介面及相依性分析作業

資安推動小組應於每年定期執行組織全景分析作業時，分析組織的各項活動，分析該活動在組織內部與其他組織活動之間的介面及相依性，以作為資訊安全管理系統執行範圍之依據。

五、決定資訊安全管理系統之範圍

資安推動小組應彙整活動間的介面與相依性、關注方之需要和期望及內部議題和外部議題之結果於管理審查會上決定資訊安全管理系統範圍是否需要調整，並將決定之結果記錄於會議紀錄中，以作為資訊安全管理系統執行範圍之依據。

六、因應風險及機會之行動作業

(一) 資安推動小組應考量內部議題和外部議題之結果及關注方之需要及期望，以決定所需因應之風險及機會，以達成下列事項：

1. 確保資訊安全管理系統達成其預期效果。
2. 預防或減少非預期之影響。
3. 達成持續改善。

(二) 資安推動小組應規劃因應風險及機會之行動並執行，以達成上述要求事項。

1. 資安推動小組可以透過風險評鑑之結果及依據關注方的需要或期望提出改善機會，並於管理審查會議中提出因應風險及機會的改善方式。
2. 資安推動小組應將關注方之需要及期望將各項行動整合及實作於資訊安全管理系統之中。
3. 資通安全管理推動小組應透過績效指標定期評估此等行動之有效性，並文件化相關資訊，以供後續評估管理系統有效性之參考。

七、修訂

本作業說明書應至少每年評估一次，確保組織全景之完整性。

柒、參考文件

無

捌、使用表單

B330-I303-01 組織全景評鑑表