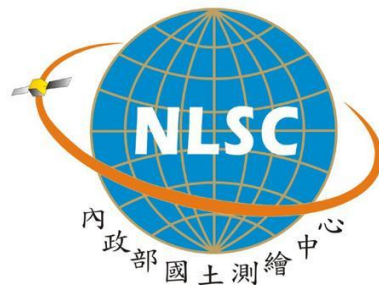

內政部國土測繪中心
資訊安全管理系統組織全景鑑別書

文件編號： ISMS-03000000

版 次： V2.01

文件日期： 110 年 10 月 8 日

機密等級： 普通



National Land Surveying and Mapping Center

文件制/修訂紀錄

制/修訂 版次	制/修訂 日期	制/修訂 說明	作 者	備 註
1.0	1031024	首版發行，配合 ISO 27001:2013 改版	蔡汶諭	
1.1	1040727	1. 增修內外部議題、關注方及營運風險。 2. 於文字內容增加關注方清冊及營運風險分析表如後附。 3. 附表關注方清冊。 附表營運風險分析表。	蔡汶諭	
1.2	1050929	1. 修正會計室為主計室。 2. 修正附表關注方清冊。	陳建男	
1.3	1080806	依現況修正各相關敘述	蕭宇辰	
V1.04	1080927	修正版次敘述	蕭宇辰	
V1.40	1090416	修正版次敘述	蕭宇辰	
V1.41	1100121	1. 新增個人資料隱私之保護列入關注方要求及新增應對措施。 2. 文件位階由四階文件修正為一階文件。	蕭宇辰	
V2.00	1100712	1. 新增文件目錄及調整文件段落格式，並新增資訊安全風險管理（ISO / IEC27005）相關規定。 2. 文件名稱「組織全景」修正為「組織全景鑑別書」。	蕭宇辰	
V2.01	1101008	考量資通訊設備異動較為頻繁，故刪除附表「關注方一覽表」及「營運風險分析表」，並另新增四階表單「關注方一覽表」及「營運風險分析表」。	蕭宇辰	
		1		

目 錄

壹、	目的	1
貳、	依據	1
參、	適用範圍	1
肆、	權責	1
伍、	管理項目	2
陸、	相關表單文件	3

壹、 目的

內政部國土測繪中心(以下簡稱本中心)為了推動資訊安全管理系統(以下簡稱 ISMS)時，能全面了解本中心全景及內外部關注方之需求與期望，以順利界定資通安全管理之方針與 ISMS 之實施規範，特訂定本「資訊安全管理系統組織全景鑑別書」。

貳、 依據

ISO27001/CNS27001 標準要求事項第 4 節「組織全景」。

參、 適用範圍

本中心全機關所提供及建立之資通訊服務。

肆、 權責

- 一、 資通安全推行小組(以下簡稱推行小組)負責審查組織全景評鑑過程記錄，擔任資通安全風險管理的決策者，決定風險因應對策。
- 二、 資訊安全管理系統工作小組(以下簡稱工作小組)負責鑑別營運目的內外部關注方及其需求與期望，協助界定 ISMS 適用範圍及分析風險的變化與新風險的產生，並執行風險因應對策之討論，提供推行小組執行審查。

伍、 管理項目

一、 組織營運目的及關注方需求與期望的鑑別。

在鑑別組織全景分析時，工作小組須參考本中心營運目的，鑑別本中心內部及外部關注方之資通安全需求與期望並採取適當之因應策略，製作「關注方一覽表」。

二、 營運風險項目分析作業

對本中心資通訊服務持續營運所需之重要項目，藉由情境描述進行營運風險分析，針對已擬定之安全控制措施及採取之因應對策，應分析其妥適性，製作「營運風險分析表」，同時確認所採取的安全控制措施或因應對策，與 ISO 27001 控制條款間之關係，彙整至「適用性聲明」。

三、 界定資訊安全管理系統適用性聲明及適用範圍與風險評鑑

「資訊安全管理系統適用性聲明」是用來依據 ISO27001/CNS27001 之附錄 A 所要求控制目標與控制措施並對應本中心各階段 ISMS 文件，工作小組須參考本中心內部及外部關注方需求與期望之議題及資通安全相關法令等，考量營運風險分析及資通訊服務範圍，選擇控制措施是否適用或不適用，並說明其原因，確認後決定 ISMS 適用範圍及驗證範圍後載明於「資訊安全管理系統政策文件」。

ISMS 適用範圍之資訊資產需進行盤點作業，後續則參考 ISO27005/CNS27005、ISO31000/CNS31000 等資訊安全風險管理原則與指導綱要，建立本中心 ISMS 風險評鑑與管理程序，識別資訊資產所存在之弱點與威脅後評估其衝擊嚴重性、發生機率及可偵測性，計算資訊資產存在之風險等級，由推行小組評估機關資源後核定可接受風險等級，

超出可接受風險等級之資訊資產則進行後續風險處理，未超出可接受風險等級仍持續依據本中心 ISMS 規範進行相關管控措施及維運。

四、 組織全景鑑別紀錄之監控和審查

針對上述執行過程與結論，均應由工作小組呈報推行小組會議討論，使得推行小組可以清楚了解本中心營運要求以及內部與外部關注方資通安全需求與期望，並確認 ISMS 適用範圍是否適當。

組織全景評鑑應至少每年審查一次，並在有任何關於營運目的改變、組織結構變更，或關注方產生新需要或期望時，增修「關注方一覽表」與「營運風險分析表」，並檢視「適用性聲明」適切性。

陸、 相關表單文件

- 一、 ISMS-02000000 資訊安全管理系統適用性
- 二、 ISMS-03000001 關注方一覽表
- 三、 ISMS-03000002 營運風險分析表