經濟部

MOEAWRA1100085

110 年度ISMS維護及驗證服務

Information Security Management System(ISMS) Maintenance and Verification Services of 2021

主辦機關：經濟部水利署南區水資源局

執行單位：創逸科技服務有限公司

中華民國 110 年 12 月

摘要

本局為配合資通安全管理法子法資通安全責任等級分級辦法附表三資通安全責任等級B級之公務機關應辦事項，受核定之2年內，全部核心資通系統導入ISO 27001 資訊安全管理系統標準，於 3 年內完成公正第三方驗證。其計畫工作項目執行分三階段說明如下：

計畫初期針對本局 8 個單位(曾管中心、阿管中心、牡管中心、甲管中心、高管中心、水文課、品管課及養護課)之ISMS執行現況訪視與差異分析，並由顧問提出與ISMS作業規範之落差及改善建議，且已由各單位根據建議事項完成改善。

計畫中期完成本局ISMS管理文件相關程序書執行及表單使用之討論與改善，在資通安全責任等級B級之公務機關應辦事項中一般使用者及主管每人每年接受 3 小時以上之資通安全通識教育訓練，IT與OT資安教育訓練共 7 場次，各單位資產盤點、風險評鑑、營運持續演練、內部稽核及管理審查等重大工作事項。

計畫後期完成本局ISMS資訊安全管理制度(Information Security Manage me-nt System)藉由台灣檢驗科技股份有限公司(簡稱SGS)第三方驗證作業通過ISO 27001 驗證並獲得正式證書。另配合「資通安全管理法」及其子法相關規定，推動政府機關導入資安治理制度，完成資安治理成熟度評估作業，以掌握整體資安防護情形。

Abatract

Southern Region Water Resources Office, Water Resources Agency, Ministry of Economic Affairs had coordinated with the Information Security Management Act and sub-laws information security responsibility level B, the attached table three requirement, within 2 years of approval, all core information and communication systems shall be imported into ISO 27001 standard, complete fair third-party verification within 3 years. The implementation of project was divided into three stages and explained as follows.

In the early stage of the project, consultants visited and analyzed the current status of ISMS implementation in 8 units of the Bureau (E.g.Zengwen Reservoir Management Center, etc.) was visited and the differences were analyzed, and the consultant proposed the discrepancies and improvement suggestions with the ISMS operation regulations.

In the mid-term of the plan, we had completed the discussion and improvement of the implementation of the ISMS management document and the use of forms, and the general users and supervisors of the public offices with the information security responsibility level B had each received more than 3 hours of information security general education training per year. The major tasks such as asset inventory, risk assessment, continuous operation rehearsal, internal audit and management review, etc. were planned to be completed.

We planed to complete the ISMS (Information Security Management System) in the latter part of the year and obtained the ISO 27001 certification through third-party verification by SGS Taiwan. In addition, in line with the provisions of the Information Security Management Act and its sub-laws, we will promote the introduction of the information security management system by government agencies and complete the information security management ma-turity assessment in order to grasp the overall information security protection situation.

結論與建議

本局資訊安全管理制度(ISMS)在今年順利通過第三方驗證作業，顯示本局在資安治理上已達一定之成熟度。但在全球資訊環境下，資訊安全的挑戰仍持續不斷，不論來自於外部的惡意威脅，還是內部的資訊使用不當，本局依然需要持續策略規劃、做好管理實務、運用技術工具，才能面對與解決各種資訊安全構面的問題。

尤其本局今年已經通過第三方驗證之單位(水文課、曾管中心、高管中心及牡管中心)，雖無不符合事項，但仍有一些待觀察事項持續矯正中，務必在明年第三方驗證前完成改善，且相同的觀察項目不可再次發生。另外，在今年內部稽核及水利署資通安全稽核的缺失，本局所有單位都務必要去了解，受稽單位也應針對未完成改善之問題儘速擬定改善計畫並完成改善，並避免發現事項再次被提出。

在本年度專案推動下，凝聚幾點共識可供作為未來持續精進ISMS之建議，區分**策略面**、**管理面**及**技術面**說明如後：

一、策略面

因應「國家資通安全發展方案(110 年至 113 年)」，對於機關資安責任、資安法規與主管機關要求，積極調整資安管理與維運重點。雖資安資源有限，但仍須符合資安法及各項法令法規的要求，當然還包括必須通過ISMS第三方驗證作業，因此考量相關利害關係方的要求與期待，執行機關風險評估與因應、落實重要營運目標持續等工作仍是重要。請本局各單位持續依照本局年度之內部及外部(水利署及SGS)稽核結果，持續矯正不符合事項，預防類似缺失不再次發生。

二、管理面

(一)**持續強化資安治理成熟度**：在國家資通安全發展方案的架構下，本局為關鍵基礎設施管理機關，負責重要的民生水資源系統控制，因此落實關鍵基礎設施資安防護基準及建構工控領域資安治理成熟度，即為時下的重點管理工作。因此，各單位須持續根據「經濟部資通安全稽核項目檢核表」及「經濟部能源領域暨水資源領域工業控制系統資安

防護基準自評檢核表」執行自我評量，完成安全控制措施之查核及改善。

(二)**加強ISMS管理標準**：資訊安全政策與目標的推動，有賴於組織全體成員的共同遵守與努力，在經過 ISMS 的 PDCA 循環後，亦可將資安目標往更嚴謹的方向調整，以彰顯 ISMS 持續強化之作為，在 ISMS 管理文件與控制措施的制訂，更需要重視管理、落實執行，以符合 ISO 27001:2013標準規範。然預期可見ISO 27001:2013也即將面臨改版，且往後工控系統將可能朝 IOT 的方向前進，至於相關的控制作法，本局可先期了解或進行策略管理的規劃。因此，本局須持續檢討並修訂本局「ISMS 四階管理文件」來符合各項法規要求且作為本局資安推動之依據，並請各單位需依照 ISMS 四階管理文件所訂之工作內容與執行週期落實資訊安全管理工作。

三、技術面

(一)**落實弱點管理，修補系統漏洞**：在資安法的要求下，執行弱點掃描、資訊安全健診等已是必要工作，定期、有效、落實弱點管理與系統修補，未來需要持續改善老舊系統既存漏洞的現況，是本局可進一步強化的目標。請各單位持續依據年度「弱點掃描」、「滲透測試」及「資訊安全健診」等各類檢測報告，完成資通系統問題修正。

(二)**實踐系統安全防護基準控制措施**：今年在行政院及經濟部主管機關的要求下，本局已完成「資安責任等級分級辦法附表十資通系統防護基準自評表」與「經濟部能源領域暨水資源領域工業控制系統資安防護基準自評表」的自評作業，因此各管理單位須針對前述自評表中不符合項目訂出改善期程，以符合系統的資訊安全條件。

(三)**日誌保存之遵循性**：在今年資安法相關子法的修正後，「資安責任等級分級辦法附表十資通系統防護基準自評表」已明確律定公務機關之核心資通系統與網路設備之日誌最短保留期限為六個月，資安事件稽查往往依賴於系統紀錄，日誌以成為後續追蹤根因與分析事件的主要來源，在現行的架構與系統功能限制下，本局須持續檢視各類系統日誌紀錄的符合度，並請所有系統維護廠商依照本局 ISMS 程序書要求，完成系統日誌紀錄的留存。