經濟部

MOEAWRA1110072

111 年度 ISMS 維護及定期追查服務

Information Security Management System(ISMS)
Maintenance and Surveillance Audit Services of 2022

主辦機關：經濟部水利署南區水資源局

執行單位：松之安資訊科技有限公司

中　華　民　國　111　年　12　月

摘要

為遵循資通安全管理法及其子法規範，協助本局落實資通安全責任等級分級辦法 B 級公務機關應辦事項等各項要求，並維持 ISO27001 資訊安全管理系統的持續有效，本計畫已於 111 年 01 月～11 月期間，陸續完成相關資安重點工作項目，包括：

- 完成本局具機房(重要系統)9 單位(曾管中心、阿管中心、高管中心、甲管中心、牡管中心、水文課、經管課、養護課及品管課)業務分析現況訪視及差異分析，並為確保 ISMS 資訊安全管理制度推動，依各課室現況與回饋意見，進行共 11 份程序文件及紀錄表單的修訂。

- 執行本局年度資訊安全管理重點工作，包含資產盤點、風險評鑑營運持續演練、內部稽核(併行個人資料保護稽核)及委外供應商查檢等資安項目，並舉行相關行前說明會議和檢討會議，加深各課室人員對 ISMS 制度與資通安全法規的認識，落實各項資安工作。

- 辦理局內 ISMS 推動及一般使用者與主管資通安全教育訓練，例如公務機關常見資安與個資事件分析教育訓練、水資源關鍵基礎設施資通安全維護教育訓練等，強化局內同仁的資安素養，認識相關的可能資安威脅與趨勢，進而提升本局資安防護能量。

- 完成本局 ISMS 資訊安全管理制度第三方定期追查作業，順利取得由 SGS 驗證公司核發之 TAF 證書，維持證書之有效性，並符合資通安全法要求。

Abstract

To comply the Regulations of Information Security Management Act and the relevant sub-laws, and continuously meet all the requirements of information security responsibility level B and ISO27001, the project assist Southern Region Water Resources Office (the WRASB) complete the following information security tasks during January to November, 2022. The tasks include:

- Completed the interviews and differential analysis with 9 departments (E.g. Zengwen Reservoir Management Center, etc.). To confirm the implementation of Information Security Management System (ISMS) and to collect the feedbacks from all departments, the project team revised in total of 11 procedure documents and record management forms.
- Executed the important ISMS tasks including properties review, risk assessment, training programs of operation, internal auditing (include personal data protection auditing), and outsourcing vendors assessment for the Office in the year of 2022. The project team hosted multiple seminars or conferences before the tasks, and hosted meetings after the events.
- Promoted ISMS protocols to users, operators, and managers. For instances, the project team hosted the training programs to prevent the frequency event analytics on information security and personal data leaks and the training programs to maintain information security of the critical infrastructures in water resources facilities. The purposes of these training programs help the users, operators, and managers increase their Iinformation security literacy, understand the possible risks.
- To continuously maintain the certification is validated and qualified of Information Security Management Act. The project has completed the third-party ISMS auditing tasks for the WRASB and received TAF certificate authorized by SGS.

結論與建議

本局因應資通安全法規新規定，於 111 年度順利通過 ISMS 第三方定期追查作業，取得 TAF 核發之證書，確保 ISMS 驗證持續有效，並由專案團隊協助進行各項年度重要資安執行事項，包括資產盤點、風險評鑑、營運持續演練、人員教育訓練等工作，可謂成果豐碩。然而，因應第三方定期追查過程中的發現，以及近期法規異動情形和我國公務機關不斷面臨的資安威脅，本局仍應持續落實 ISMS 制度的推動，強化相關資安防護作業，並促進局內各單位遵循資安規範，以確保轄管關鍵基礎設施和重要資通系統的防護，達到保障經濟、民生穩定的重要目標。

評估本年度專案執行之各項工作與成果，建議局內相關單位及承辦人員除持續精進資安管控作為外，並需留意以下建議內容。

- 有關 111 年度執行之內部稽核與第三方定期追查作業，相關稽核發現之短期矯正對策雖皆已完成，各單位仍須持續留意管控措施的落實，以維持 ISMS 制度的有效，並於 112 年度檢視、確認有無類似狀況的發生，達到預防及降低風險的成效。另針對 110~111 年內、外稽發現與建議事項綜整如附錄十六所示。

- 因應資通安全管理法於 110 年 8 月 23 日的修訂，經濟部業已於 111 年 9 月 16 日正式發佈「經濟部能源及水資源領域工業控制系統防護基準」修正版(經資字第 11104884320 號 令)，由於本局轄管之關鍵基礎設施工業控制系統皆須遵循此防護基準要求，後續仍需持續評估相關規範的異動狀況，並強化各項管控措施作為，以符法遵。有關經濟部版防護基準新舊版本差異說明，分列如下：

  1. 存取控制構面：「帳號管理」及「遠端存取」控制措施內容有修訂；其中需留意「遠端存取」將 2 項原為中、高等級項目調整為普等級即需遵守。

2. 事件日誌與可歸責性構面：整個構面將「稽核」一詞修訂為「事件日誌」；而「記錄事件」控制措施新增 1 普級項目，明訂日誌記錄需保留至少六個月以上。

3. 營運持續計畫構面：整個構面將「測試」一詞修訂為「演練」，使營運持續演練之作法更具彈性。

4. 鑑別與識別構面：「身份鑑別管理」控制措施進行相關字詞修訂，並刪除原「強制新密碼最少變更字元數」之要求，以貼近實務作業現況。

5. 系統與通訊防護構面：「資料儲存之安全」控制措施考量儲存作業多元性，允許加密作業之外之適當儲存方式，並明確定義包含重要組態設定檔案在內之相關具保護需求標的。

6. 系統與資訊完整性構面：調整「操作與維護日誌資訊留存」控制措施之字詞，以與「事件日誌與可歸責性構面」中所提之「事件日誌」有所區隔。

- 目前本局 ISO27001 驗證範圍為三處管理中心之閘門檢控系統、水工圖控系統和水工機械操作系統，然而依據水利署的規定，核心工控系統範圍已將放流警報系統納入，屬需通過公正第三方驗證之範疇，未來必須規劃相關導入與認證作業，以滿足上級機關之規定。

- 新版 ISO27001:2022 已於 111 年 10 月 25 日正式發佈，面對未來的轉版需求(預計為 113 年再次重新驗證時轉版)，在後續 ISMS 的執行上，需積極評估與新版規範的差異，並調整必要程序規定，強化新控制措施的遵循作為，以確保轉版作業的順利推展。有關 ISO27001:2013 與 ISO27001:2022 差異說明，分列如下：

  1 資安控制措施從 ISO27001:2013 的 14 大類(A.5~A.18)114 項，修訂為 ISO27001:2022 的 4 大類(分別為 Organization, People, Physical 與 Technological)共 93 項。

2　與 ISO27001:2013 相比，ISO27001:2022 共計有 11 項新增控制項目，包括：

- 5.4 威脅情資(Threat intelligence)
- 5.23 雲端服務資訊安全(Information security for use of cloud services)
- 5.30 資通訊技術營運持續整備(ICT readiness for business continuity)
- 7.4 實體安全監視(Physical security monitoring)
- 8.9 組態管理(Configuration management)
- 8.10 資訊刪除(Information deletion)
- 8.11 資料遮罩(Data masking)
- 8.12 資料外洩防護(Data leakage prevention)
- 8.16 監視活動(Monitoring activities)
- 8.23 網站過濾(Web filtering)
- 8.28 安全程式碼撰寫(Secure coding)
- 原屬 ISO27001:2013 之 57 項控制措施，於 ISO27001:2022 已整併為 24 個控制措施，詳細內容請參考文獻十二。

- 無論是資通系統防護基準或工控系統防護基準，針對各類系統之日誌紀錄留存，皆已規定需達到 6 個月以上，且需考量定期檢視作業； 由於此項規定涉及各系統日誌紀錄留存規劃和必要資源的安排，亦關係承辦人員日常維運時的落實檢視，因此仍需持續追蹤、檢視各系統的執行情況，要求承辦人員或委外廠商依程序規範，使相關日誌紀錄留存和定期檢視的作為能夠確實實施。

上述各項建議宜作為本局後續推行 ISMS 制度與遵循法令法規規範之重要事項之一，相信在局內同仁與委外廠商的協力推動下，應該順利推動，落實各項管控措施，符合資通安全管理法之要求，並確保本局核心業務的資安防護，保障區域的民生經濟發展。