經濟部

MOEAWRA1090184

109年資訊安全管理系統(ISMS)導入輔導專案

Information Security Management System(ISMS) Introduction Project of 2020

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　109　年　12　月

摘要

經濟部水利署南區水資源局奉行政院核定為資通安全責任等級B級公務機關，為符合資通安全管理法及其子法資通安全責任等級分級辦法之B級公務機關應辦事項規定，透過本案建置資訊安全管理系統(ISMS)，並落實相關管控制度及程序。

計畫初期透過七個單位之現況訪視與差異分析，了解機關現況與需求，提供資通安全維護計畫調整建議，並協助機關調整適用性聲明與資訊安全政策檢視，同時協助機關調整資訊安全管理程序文件，並藉由導讀方式提升機關人員認知，作為後續實作基礎；以及完成年度資安宣導訓練。

計畫中期透過資產盤點與風險評鑑訓練，建立機關人員實作能力，並協助機關檢視資訊系統分類分級且提供調整建議；接著協助機關識別核心資通系統，完成營運衝擊分析作業，並依據分析結果擬定營運持續計畫與年度資訊安全營運持續演練作業，供機關據以進行演練，並配合機關執行汛期前資安檢核作業；以及協助機關完成年度資訊安全管理制度有效性量測作業。

計畫後期進行內部稽核教育訓練，建立機關人員稽核能力，並協助機關擬定內部稽核計畫、執行內部稽核作業及提供內部稽核報告，依據稽核發現進行矯正與預防作業，以完備資訊安全管理制度；且協助機關建構與優化委外管理程序，並協助機關執行兩家委外供應商資安稽核，以減少發生資安事件與衝擊之機率。另協助機關辦理資安治理成熟度評估訓練與紀錄討論，以提升機關整體資安防護機制。最後，協助機關擬定管理審查項目，以利機關完成管理審查會議，檢討年度資訊安全管理制度執行成果，作為下一個資訊安全執行循環(PDCA)之參據；並邀請第三方驗證公司進行ISO 27001 預評作業，藉由第三方驗證機構之預評服務，檢視顧問輔導之有效性，及早進行矯正與預防，且可使機關同仁提前有接受稽核之經驗，了解第三方驗證之稽核模式。

期透過本案協助機關建構完善之資訊安全管理系統核心模型(PDCA)，並落實相關管控制度及程序，以協助機關提升資安防護機制與管理制度，與期通過 110 年第三方驗證正評作業取得ISO 27001 證書。

Abstract

The Southern Region Water Resources Office, WRA, MOEA, was designated as the government agency with Level-B cyber security responsibility. To conform with the requirements set for Level-B government agencies by the Regulations on Classification of Cyber Security Responsibility Levels and its parent legislation the Cyber Security Management Act, an Information Security Management System (ISMS) will be deployed through this project along with the associated controls and procedures.

The project will begin by establishing the current situation and requirements of the agency through the inspection and differential analysis of seven units. Recommendations will be made on the adjustments to the cyber security protection plan and the agency given assistance on making adjustments to its Statement of Applicability and review of cyber security policy. The agency will also receive assistance on adjusting its cyber security management procedure documentation. Guidance will be provided to enhance awareness among agency personnel and pave the way for subsequent implementation. Annual cyber security education and training will be carried out as well.

The interim phase of the project will conduct an asset inventory and risk assessment training to cultivate the hands-on skills of agency personnel, help the agency review its information system categories and levels, and provide suggestions on adjustments; next, the project will help the agency identify its core information systems, conduct a business impact analysis and use the findings to draw up the business continuity plan and annual cyber security persistent exercises that the agency can use for training. The agency will also receive support on carrying out an information security review before the typhoon season and on completing its annual measurement of cyber security management performance.

The final phase of the project will involve internal audit training to establish an audit capability within the agency. The agency will also receive assistance on developing an internal audit plan, conducting internal audits and preparing internal audit reports. The audit findings will serve as the basis for corrective and preventive actions that enhance the integrity of the cyber security management system. The agency will also receive help on establishing and optimizing its contractor management procedure and for conducting cyber security audits on two contractors to reduce the risk of cyber security incidents and impacts. The agency will also receive assistance on the hosting of cyber security governance maturity evaluation training and discussions that enhance the overall cyber security protection of the agency. Finally, the agency will receive assistance on formulating the contents of the management review. This will allow the agency to hold management review meetings on the implementation of cyber security management for the year and provide a reference for the next cyber security implementation loop (PDCA); A third-party certification body will also be invited to conduct an ISO 27001 pre-evaluation. The pre-evaluation by a third-party certification body

will be used to review consulting effectiveness for early correction and prevention. This will also provide agency employees with experience on undergoing audits and understand the audit model of third-party inspectors.

The goal of this project is to assist the agency with building a comprehensive ISMS core model (PDCA). Associated controls and procedures should also be implemented to help the agency improve its cyber security mechanism and management system. We aim to complete the third-party certification process and obtain the ISO 27001 certificate in 2021.

結論與建議

一、結論

經過109年一整年資訊安全管理制度的實施，在機關各單位的全力配合與顧問的協助下，已經將整個資訊安全管理系統實施過一個完整循環，亦透過顧問協助辦理內部稽核活動，將可再優化的實務面控制措施發掘與呈現，並與顧問公司共同研擬改善計畫作為，最後再彙整各單位對於管理制度可再調整的部份，藉由管理文件修訂的方式，讓相關管理制度可以更明確、更容易理解，也讓各單位更能落實相關作業。達成效益與成果如下，

(一) 完成資安作業流程建置，降低機關資訊安全風險，完善機關資訊安全管理系統機制。

(二) 完成B級公務機關應辦事項，符合資通安全管理法及其子法要求，強化機關整體資訊安全保護。

(三) 完成ISMS教育訓練，提升人員資訊安全認知與專業技能。

依據本案需求書之各工作項目，產出執行成果如下工作項目與執行成果對照表。

工作項目與執行成果對照表

工作項目		執行成果	佐證
0			
0.1	現況檢視	1. 現況檢視報告 2. 各單位改善情形	附件 1
A	資安作業流程建置		
A.1	適用性聲明與資訊安全政策檢視與調整建議	1.文件修訂建議表 2. 程序書修訂內容說明	表 2-3 表 2-8
A.2	年度資產盤點與風險評鑑作業	1.資通系統清冊 2. 各單位風險評鑑報告	表 2-4 附件 2
A.3	資訊系統分類分級檢視與調整建議	資通系統清冊	表 2-4
A.4	營運衝擊分析作業	1. 衝擊分析檢視說明與建議 2. 各單位營運衝擊分析統計	附件 3 圖 2-3 各

工作項目		執行成果	佐證
			單位營運衝擊分析統計
A.5	年度資訊安全營運持續演練作業	表 2-6 持續演練作業管制表	表 2-6
A.6	矯正與預防作業	內部稽核發現問題彙整表	表 4-2 內部稽核發現問題彙整表
A.7	年度資訊安全管理制度有效性量測作業	各單位有效性量測結果統計表	表 2-7
A.8	資通安全維護計畫調整建議	資通安全維護計畫	附件 13
A.9	資訊安全管理程序與文件調整建議	1. 文件修訂建議表 2. 程序書修訂內容說明	表 2-3 表 2-8
A.10	辦理資安治理成熟度評估	資安治理成熟度評估資料	附件 4
A.11	提供 ISMS 工具平台	ISMS 管理工具說明文件	附件 5
A.12	發展資安行事曆	資安行事曆	附件 6
B	ISMS 教育訓練		
B.1	辦理資訊安全管理制度認知與實施教育訓練至少 5 場次	1. 資訊安全管理作業說明會 2. 資訊系統分級、資產盤點與風險評鑑作業訓練 3. 資安認知宣導課程 01 4. 營運持續管理 5. 資安認知宣導訓練 02 6. 內部稽核教育訓練	附件 7
B.2	提供 2 人次 ISO 27001 主導稽核員證照培訓課程	1. 課程通知書 2. 上課證明及證書	附件 8
C	內部稽核與管理審查		
C.1	依據 ISO 27001 審查現有各項作業執行記錄	內部稽核查驗表	附件 9
C.2	稽核前提供內部稽核計畫	內部稽核計畫	附件 9

工作項目		執行成果	佐證
C.3	稽核後提供內部稽核報告	1. 圖 4-2 內稽結果統計 2. 內部稽核發現問題彙整表 3. 內部稽核總結報告書	圖 4-2 表 4-2 附件 9
C.4	協助擬訂管理審查項目	1. 協助擬訂管理審查議題 2. 彙整管理審查資料	P.4-4
C.5	辦理委外供應商稽核作業 2 家	1. 委外供應商稽核計畫 2. 委外供應商稽核報告 3. 委外供應商稽核查驗表	附件 10
C.6	提供 ISO 27001 預評	1. 預評稽核報告	附件 11
D	工作會議		
D.1	期初簡報暨工作執行計畫書審查會議	期初簡報暨工作執行計畫書審查會議意見及辦理情形	附件 12
D.2	期中審查會議	期中報告書審查會議意見及辦理情形	附件 12
D.3	期末審查會議	期末簡報暨成果報告書(初稿)審查會議意見及辦理情形	附件 12

二、建議

然管理制度建制完成後，下階段目標是資安管理成熟度的深化，同時，在資通安全管理法的要求下，貴局須進行資訊安全管理制度第三方稽核，並取得證書，這是更艱難的考驗，同時也是驗收貴局一年來配合執行的成效，故針對貴局後續資訊安全管理作業之建議如下：

制度面向	辦理項目	辦理說明	建議
管理面	資通系統分級及防護基準	已建立制度，每年至少檢視一次資通系統分級妥適性。	建議參考資安行事曆時程執行作業。
	內部資通安全稽核	已建立制度，每年辦理一次。	建議參考資安行事曆時程執行作業。
	業務持續運作演練	已建立制度，全部核心資通系統每二年辦理一次。	建議參考資安行事曆時程執行作業。
	資安治理成熟度評估	已建立制度，每年辦理一次。	建議參考資安行事曆時程執行作業。

制度面向	辦理項目	辦理說明	建議
技術面	網站安全弱點檢測	全部核心資通系統每年辦理一次。	建議可從官網開始執行，循序漸進地將對外網站納入執行標的。
	系統滲透測試	全部核心資通系統每年辦理二次。	此技術是模擬駭客進行無害式攻擊，建議以對外IP或URL為標的。
	資通安全健診	每二年辦理一次。	建議除了IT資安健診，可考慮將OT資安健診納入規劃。
訓練面	一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。	建議透過通識課程與貴局資安管理規範進行結合，以提升機關人員之資安認知。
	資通安全專業證照	已取得兩張ISO 27001 Lead Auditor 證照。Lead Auditor 相關證照須提供當年度至少 2 次實際參與該證照內容有關之稽核經驗證明。	建議可與同性質機關協調互相參與彼此之內部稽核活動，以達證照有效性。