經濟部

MOEAWRA1120077

112年度ISMS維護與定期追查及工業控制系統(ICS)威脅偵測機制與資安演練

2023 Information Security Management System (ISMS) Maintenance and Industrial Control System (ICS) Threat Detection Mechanism and Security Drills Services

主辦機關：經濟部水利署南區水資源分署

執行單位：天雷科技有限公司

中華民國 112 年 12 月

摘要

經濟部水利署南區水資源分署(以下簡稱本分署)所轄關鍵基礎設施場站為我國水資源領域重要關鍵基礎設施場站，為遵循資通安全管理法暨相關子法規範，並確保核心工業控制系統防護符合「經濟部能源及水資源領域工業控制系統資安防護基準」各項控制措施之要求，本分署從政策面、管理面及技術面的防禦部署，並驗證及檢測相關資訊安全管理、防護機制的有效性，以維護和強化本分署與轄管各關鍵基礎設施的資安防護，持續提升本分署轄管水資源關鍵基礎設施場域面對可能資安事件衝擊的應對能力，建構嚴密之資通安全防護結構。

本計畫之兩大重點工作包含「ISMS 維護與定期追查」及「工業控制系統(ICS)威脅偵測機制與資安演練」，服務團隊已於 112 年 01 月至 11 月期間，依工作執行計畫書進度陸續完成計畫相關工作項目，包括：

- 完成本分署具機房(重要系統)8 單位(曾管中心、阿管中心、高管中心、甲管中心、牡管中心、水文科、品管科及人事室)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，依各科室現況與回饋意見，進行共 5 份程序文件及紀錄表單的修訂。
- 執行本分署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，加深各科室人員對 ISMS 制度與資通安全法規的認識，落實各項資安工作。
- 辦理分署內 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，強化分署內同仁的資安素養，認識相關的可能資安威脅與趨勢，進而提升本分署資安防護能量。

- 完成本分署 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。
- 維護曾管中心及牡管中心之可視化網路監測平台，已提供第一季至第三季的威脅分析季報，並於 112 年 07 月 14 日舉辦可視化監測平台教育訓練。
- 已建置阿管中心、高管中心及甲管中心 3 個場域之可視化網路監測平台，持續蒐集主機狀態資訊與系統安全日誌。
- 已執行曾管中心及牡管中心 2 個場域之工控資安健診，已分別於 112 年 05 月 19 日與 112 年 06 月 26 日提交曾管中心與牡管中心的資安健診報告。
- 針對紅隊演練作業所需之情境場景進行評估，包含與牡丹水庫管理中心管理和維運人員進行訪談，並進行針對場域實體安全與內部網路安全進行評估，已於 112 年 06 月 30 日完成並提交紅隊演練執行計畫書。
- 已完成本年度牡丹水庫管理中心紅隊演練作業，過程中發現相關的可能脆弱點與風險，並提出對應的矯正措施，進而提升本分署資安防護能量。

Abstract

Southern Region Water Resources Branch, Water Resources Agency, Ministry of Economic Affairs is a fundamental infrastructure of water resources in National water resources domain. To comply the regulations of Information Security Management Act. and the relevant sub-regulations, Southern Region Water Resources Branch (a.k.a. WRASB) deploys comprehensive defending solutions including policy, management protocols, and technology to make sure that the defends of main industrial control system is qualified of the Information Security Protection Specifications for Industrial Control Systems in the Energy and Water Resources Fields of the Ministry of Economic Affairs. Southern Region Water Resources Branch constantly validates and examines the efficiency of information security management and defending mechanisms in order to maintain and enforce the critical infrastructure in WRASB and its ruled locations. One of the Branch's missions is to constantly improve the capability of reaction to any possible cybersecurity events/risks on all critical water resource infrastructures.

The tasks in this project include "Information Security Management System (ISMS) Maintenance" and "Industrial Control System (ICS) Threat Detection Mechanism and Security Drills Services". The project team has completed the relevant task items during January to November, 2023. The completed tasks include:

- Completed the interviews and differential analysis with 8 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 5 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 2023. 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.
- Maintained visualizable monitoring platforms at Zengwen Reservoir Management Center and Mudan Reservoir Management Center.
- Established visualizable monitoring platforms at Agongdian Reservoir Management Center, Gaoping River Weir Management Center and Jiaxian Weir Management Center. The project team not only constantly managed the machines' status and collected system's security logs, but also hosted training programs on visualizable monitoring platforms to fulfill the information security requirements.
- Completed the Services of Information Diagnosis of Zengwen Reservoir Management Center and Mudan Reservoir Management Center for the year of 2023.
- Evaluated the scenarios and requirements for the Red Teaming Assessment. The project team focused on the interviews with managers and operators at Mudan Reservoir Management Center and evaluated the security risks in the physical locations and internal network environment.

- Completed the Red Teaming Assessment of Mudan Reservoir Management Center for the year of 2023. The project team discovered a few possible weak points and security risks during the training. The project team proposed the actions to fix the possible risks and further achieve the improvement of information security in Southern Region Water Resources Branch.

結論與建議

本分署因應資通安全法規定，於 112 年度順利通過 ISMS 擴大驗證範圍之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，包括現況訪視、資產盤點、風險評鑑、營運持續演練、人員教育訓練、工業控制系統(ICS)威脅偵測機制與資安演練等工作，可謂成果豐碩。

本計畫自 112 年 01 月執行至今，各項工作皆按既定之期程順利執行，計畫團隊執行過程中適時與本分署溝通協調，並依據相關回饋之意見調整執行細節，達成計畫相關目標。目前已於曾管中心與牡管中心建置可視化網路監控平台，蒐集工控主機設備狀態與系統日誌，透過可視化介面加強提供管理人員即時掌握各設備之資源與運轉狀態，進而確保系統持續營運。

本分署此次在牡丹水庫管理中心執行紅隊演練，透過紅隊演練形式驗證及檢視現有資訊安全管理及防護機制之有效性，提出持續改善及管理方式，強化本分署所轄水資源場域資訊基礎設施防禦能量。

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，本分署仍應持續落實 ISMS 制度的推動，強化相關資安防護作業，並促進分署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，建議分署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 112 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 113 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。

- 因應資通安全管理法於 110 年 08 月 23 日的修訂，經濟部業已於 111 年 09 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)，由於本分署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。

- 目前本分署 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，112 年亦依據水利署規定將核心工控系統範圍納入放流警報系統，並通過公正第三方驗證。後續

也將規劃其餘兩處管理中心之相關導入與認證作業，以擴大資安防護之範圍。

- 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 ISO 27001:2022 新增之控制措施與預計增修之程序書如下表所示：

項次	控制措施編號	控制措施名稱	預計增修之程序書
1	6.3	變更之規劃	2-A080-1-00_資訊資產管理程序書
2	A.5.7	威脅情資	2-A090-1-00_資訊管控程序書、新增對應之 3 階作業標準書
3	A.5.23	使用雲端服務之資訊安全	2-A150-1-00_資訊委外管理程序書或不適用
4	A.5.30	營運持續之 ICT 備妥性	2-A170-1-00_持續性管理作業程序書
5	A.7.4	實體安全監視	2-A111-1-00_實體環境安全管理程序書
6	A.8.9	組態管理	2-A090-1-00_資訊管控程序書
7	A.8.10	資訊刪除	

項次	控制措施編號	控制措施名稱	預計增修之程序書
8	A.8.11	資料遮蔽	
9	A.8.12	資料洩漏預防	
10	A.8.16	監視活動	2-A112-1-00_設備維護及安全管理程序書
11	A.8.23	網頁過濾	2-A090-1-00_資訊管控程序書
12	A.8.28	安全程式設計	2-A140-1-00_系統開發與維護程序書 2-A150-1-00_資訊委外管理程序書

- 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。
- 5 個管理中心之可視化監測平台已建置完成，透過平台可監測工控環境主機狀態與日誌蒐集呈現，建議管理人員仍須定期登入平台檢視主機設備狀態，並觀察相關主機安全日誌是否有異常行為。另，本分署已將各管理中心之放水警報系統納入核心工控系統，未來將考量納入可視化監測平台之需求。

- 可視化平台現階段可監測場域主機資源狀態與蒐集場域主機日誌，並將相關資訊呈現於網站平台畫面，供本分署場域維運人員監測場域主機狀態。建議後續可持續優化可視化平台，針對場域主機所蒐集之資訊進行分析，提供更多元的資訊安全監測資訊，或可透過白名單限制來源 IP 存取可視化平台，提升平台安全性。
- 有關 112 年度執行牡丹管理中心紅隊演練作業，相關演練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，後續也須持續監測場域營運狀態與安全性，並強化各項管控措施作為，達到預防及降低風險的成效。
- 因應 113 年度 ISO 27001:2022 轉版驗證，本分署規劃預計推動期程如下表:

規劃執行時間	辦理內容
112 年 12 月	相關新版程序文件討論
113 年 01 月	新版程序文件修訂完成
113 年 02 月	辦理第 1 次管理審查會議
113 年 03 月	完成資訊資產盤點
113 年 04 月	完成風險評鑑作業
113 年 05 月	完成營運持續管理作業
113 年 06 月	完成各單位內部稽核作業
113 年 07 月	辦理第 2 次管理審查會議
規劃執行時間	**辦理內容**

113 年 09 月	辦理ISO 27001:2022 第三方驗證

上述各項建議宜作為本分署後續推行 ISMS 制度與遵循法令法規規範之重要事項之一，相信在分署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，並確保本分署核心業務的資安防護，保障區域的民生經濟發展。

南區水資源分署出版品版權頁資料

112年度ISMS維護與定期追查及工業控制系統(ICS)威脅偵測機制與資安演練

出版機關：南區水資源分署
地址：715004 臺南市楠西區密枝里70號
電話：(06) 575-3251-9
傳真：(06) 575-4578
網址：https://www.wrasb.gov.tw
編著者：天雷科技有限公司
出版年月：112年12月
版次：初版
定價：新臺幣500元
EBN：10112M0017

電子出版：本書製有光碟片
聯絡資訊：南區水資源分署
電話：(06) 575-3251~9

專業　　創新　　永續

經濟部水利署南區水資源分署

曾文辦公區

地址：715004臺南市楠西區密枝里70號

網址：https://www.wrasb.gov.tw

總機：(06)5753251

傳真：(06)5754578

燕巢辦公區

地址：824002高雄市燕巢區工程路1號

電話：07-6166137

傳真：07-6166046

EBN: 10112M0017

定價: 新臺幣 500 元