來自 BS-7799 的肯定－自來水公司（SOC）安全監控中心

壹、前言

台灣省自來水公司（以下簡稱本公司）為建立全天候資訊安全監控機制，針對重要網路設施、資訊系統提供更有效的安全防護，以落實資通安全管理政策。於 2005 年規劃資安監控中心(Security Operation Center - SOC)併同導入與建置資訊安全管理系統（Information Security Management System - ISMS），期藉安全監控防護網的建立，提供駭客、病毒事件預警及通告功能，隨時掌握本公司重要伺服主機、網路、防火牆、入侵偵測系統之資訊安全狀況，提昇整體資訊安全防禦能量；並為確保業務之持續營運，促進本公司內部資訊處理安全，降低資料外洩之風險，亦委請資安廠商提供必要之 7*24 不中斷同步監控及諮詢顧問服務，進行本公司資訊系統之安全檢測、安全防護規劃、評鑑及取得 BS7799 國際安全認證，以落實資通安全管理政策目標。

貳、SOC 建置及 ISMS 導入

鑑於資通安全工作為未來必然之趨勢，囿於有限人力、經費，本公司採整體規劃分階段實施原則，第一階段以建立「資安監控中心(SOC)」為工作目標，藉由「資安監控中心(SOC)」與重點局部範圍之資訊安全管理系統建立，得以累積實際導入與運籌經驗並能循序擴大範圍至整體資訊業務之範疇，同時透過持續資安觀念及教育宣導課程，亦可有效紓解同仁的抗拒感與疑慮。

本公司第一期規劃實施範圍為：

A. 資安監控中心（SOC）建置。
B. 委外安全監控（7*24）小時資安事件偵測、監控處理、安全警示通報。
C. 安全監控中心（SOC） BS-7799 驗證輔導。

一、 資安監控中心(SOC)建置

（一）規劃：

規劃初期從「展示」、「顯示」、「標示」三方面多元化蒐集相關資訊：

展示方面：包含監控空間、監控台型式、操作機位、照明，也併同考量電力、網路、空調、裝潢、參訪動線等細節。

顯示方面：包含監控畫面雛型、投影方式（前投、背投、液晶螢幕）、環境監控、資訊資產管理、網路即時監控畫面等。

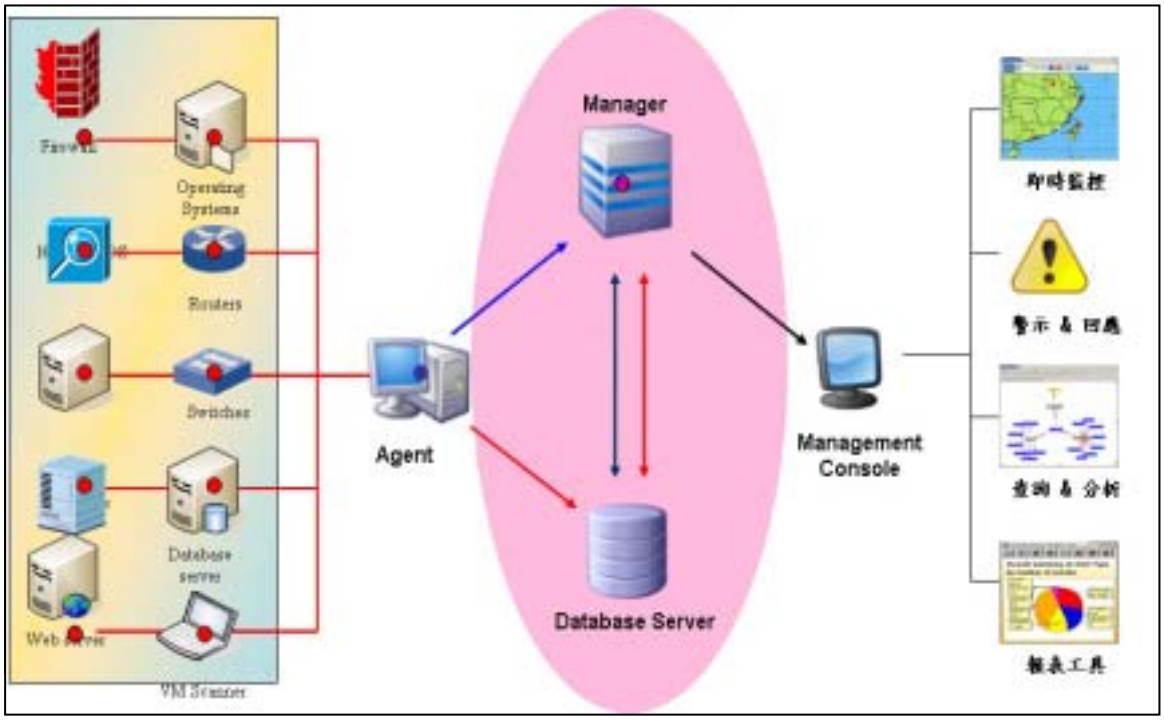
標示方面：包含燈箱選擇、標準作業流程、監控架構、宣導標語等掛圖。

（二）實體建置：

基於資安監控中心實體環境安全考量，規劃增設獨立門禁管制區域，採用刷卡感應系統實施人員進出管制。透過數位監視系統，全程遠端安全監控門禁、電力、空調、溫溼度等系統。資安監控中心為隔離與作業無關人員，同時於管制區域加裝落地窗及窗簾，保護伺服主機、網路、防火牆、入侵偵測系統所顯示之資訊。

（三）平台建置：

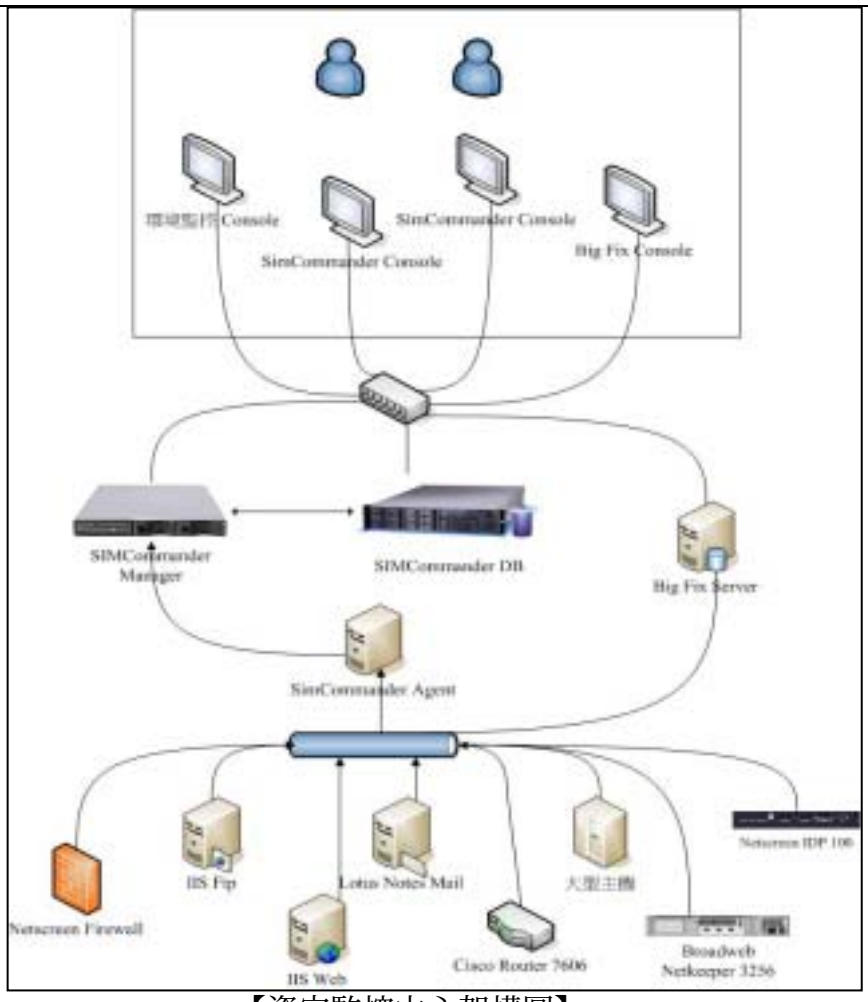
本公司資安監控中心(SOC)所採用的管理平台 SIMCommander 為中文化操作介面，符合 Unicode 規範的資安事件管理軟體平台，可執行集中化資安監控及全方位安全管理，將不同設備的 events/logs（如：防火牆、入侵偵測、防毒應用程式、路由器、交換器、作業系統、資料庫及其它應用程式等），進行資料收集、關聯分析，並以視覺圖形化方式呈現資安現況等，將龐大的資安資料透過親和力的介面呈現，監控人員能快速而有效地察覺資安異常狀況，立即執行異常事件處置，自 2005 年 12 月上線運作以來，已初步獲得實際監控效果。



【 SIMCommander 架構示意圖】

SIMC 包含重要元件，分述如次：

- Agent – 主要負責接受來自網路及安全設備的事件，收到事件後會執行兩個步驟：第一、根據自訂的過濾政策將不需要的事件過濾。第二、將來自不同設備不同格式的事件轉換成同一格式事件，這就是所謂的事件正規化，正規化後的事件可以讓 SIMCommander 簡單地了解並且將來自不同設備的事件對應成統一格式的事件，同時利用 Agent 上制定的過濾政策依各控管區域做不同設定，可達分層管理各區域資安事故，具逐級過濾及通報功能。
- Manager – Manager 是 SIMCommander 的政策和設定的控管中心，會執行來自 Console 的政策和指令並且將資料庫處理的資料傳給 Console，同時分析和關聯來自不同設備的事件，它的混合式關聯引擎結合了 Statistical、Rule-based 及 Machine-learning 等方法，有效的發掘網路攻擊事件。
- Management Console – 提供安全管理者一個完整並容易上手的使用者管理介面，管理者可以輕易地使用這個介面來進行監控、分析、警告及產生資安報表。



【資安監控中心架構圖】

目前本公司主要的資安設備如 Broadweb Netkeeper 3256、Netscreen IDP 100 以及 Netscreen Firewall 的資安事件陸續完整蒐集進入安全管理平台；其他重要主機如

IIS Ftp Server, IIS Web 以及 Lotus Notes Mail 等的應用系系統紀錄檔，也正常匯入安全管理平台集中監看、控管。

（四）、標準作業流程(SOP)：

資安監控中心(SOC)的監控作業中，雖然平台本身扮演非常重要的角色，但如果缺乏標準作業流程的輔助，平台本身仍然不足以顯現其效益，標準作業流程除能協助監控人員依照標準化，快速處理既定工作，亦能成為新進人員教育訓練教材，不致因為人員更迭，造成管理上之困擾，主要標準文件如次：

1、資安監控中心組織文件

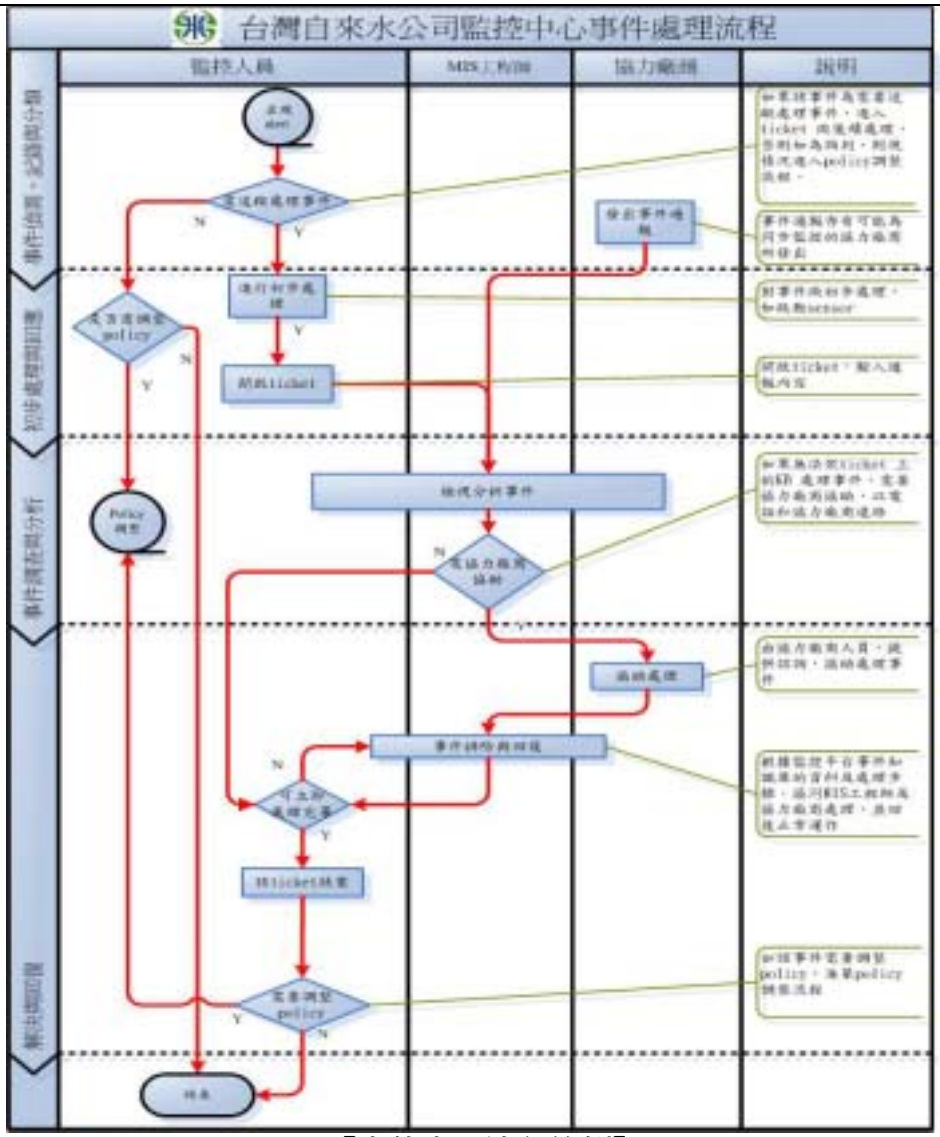
包含監控中心組織及其所屬職責，詳述監控中心日常營運任務劃分，重大事件通報、處置、復原機制及編組。

2、日常監控標準作業程序

包含監控人員每日所需執行工作及管理階層稽核機制。

3、事件處理作業程序

包含監控人員於監控平台上發現新資安事件，研判通報標準、通報處理、通報結案的過程，透過完整通報流程，落實威脅管理機制。



【事件處理流程範例】

（五）協同維運

一般資安監控中心維運管理模式劃分為委外安全管理與自建資安監控中心(SOC)，至於選擇何種方式，端視公司內的資源及業務性質而定。

協同維運是一種合作經營的模式，既是委外亦是自建，也就是單位自建資安監控中心，基於人力、技術無法有效執行全天候(7x24)監控作業，特委請資安監控廠商輔助監控，汲取專業監控技術，彌補初期資安處理的能力不足，逐步於技術移轉及經驗交流中厚植資安監控處理能力。

（六）效益：

服務項目	服務效益
全天侯資安事件監控	- 即時掌握威脅事件的發生，並由資安專業人員進行分析及研判，過濾出真正的威脅及異常事件。
即時威脅事件的中文通報	- 在最短時間內接到經過專業分析過濾後的事件通報、詳細的說明及解決方案。 - 採全中文的說明，可在最短的時間內瞭解通報內容。 - 通報方式採電話、傳真及電子郵件。 - 通報時間於 30 分鐘內完成。
重大資安通報事件緊急處置作業	- 立即啟動重大資安通報事件緊急處置作業，進行緊急防禦流程，以避免危害的擴大。
威脅事件的處置追蹤、協助	- 用來確保威脅事件經過確認及改善的措施，才能持續降低資安風險。 - 針對事件的追查、修復及防禦應提供協助。
每月定期事件報表，及通報報表	- 獲得定期性資安事件的統計分析結果，可充份充分追蹤及掌握長期性的資安動態。 - 呈現安全監控的成效。

二、 ISMS 導入效益

（一）預算花在刀口上

透過精確的風險評鑑，能有效了解單位內風險最大的資產。在預算的編列使用上，可針對這些重要資產，購買相關的設備或服務有效降低單位內整體風險。

（二）循序漸進導入資安管理系統

面對資訊安全千頭萬緒，常常有不知如何開始的痛，或者只能單點單點的看。無法全面對資訊安全做有效控管。透過 ISMS 之 PDCA（Plan Done Check Action）的流程，單位內可以先從風險評鑑中風險最大的資產開始管理起，一步一步透過不斷的計畫、實行、評估、改善。可藉由不斷完成一小部份的控制項，聚少成多至最後有效彙整達成組織的資訊安全管理目標。

（三）人的管理

在導入 ISMS 的過程中，有非常多的不適應。尤其是多年來的習慣要改變可說是非常辛苦的事。但透過各項流程的要求，以及不斷對主管以及一般人員施以教育訓練，對資訊安全本身、組織資安政策以及一般個人該注意事項不段重復提醒，已逐漸讓資訊安全概念落實於員工日常作業行為之中。例如個人密碼帳號

的管理，以及螢幕保護程式的設定，都是明定於程序中，並在教育訓練中予以考核評鑑確認成效。

（四）建立各項標準作業程序，擬訂有效改善方案

ISMS 主要是針對制度面來建立。不管針對系統安全、網路安全、實體安全、人員訓練或資產管理皆擬有相對應的標準作業程序。也就是說，藉由這個機會，重新由制度面全面將資訊安全的各個層面檢視一次，並訂定標準，要求大家遵守，再藉由不斷的執行以及審查，來確定各個程序的有效性。

參、未來規劃

資訊安全和 ISMS 是長期而且必須持續進行的工作。本公司未來將針對風險評鑑結果風險較高系統，陸續規劃有效因應的安全管控措施，以降低系統風險至可接受程度。透過資安監控中心(SOC)協同維運的運籌模式，汲取專業廠商監控、歸納、研判與追蹤處理資安事件技術能力，逐步於技術移轉及經驗交流中厚植本公司資安監控處理機制，持續降低資安風險繼而充份掌握整體的資安狀態，以期發揮資安監控中心(SOC)的具體成效。

（本文由台灣省自來水公司資訊中心工程員曾沛聰 提供）