



102年度
雲端資安防護整合服務委外服務案
SOC參考指引
(V2.0)

國家資通安全會報技術服務中心
中華民國102年7月

報告摘要

報告名稱	SOC 參考指引(V2.0)
資訊等級	<input type="checkbox"/> 機密 <input type="checkbox"/> 密 <input type="checkbox"/> 內部使用 <input checked="" type="checkbox"/> 普通
相關撰稿人	張京文、紀佳妮、方耀宇、黃博禮
閱讀對象	<input checked="" type="checkbox"/> 一般主管 <input checked="" type="checkbox"/> 資安人員 <input checked="" type="checkbox"/> 資訊人員 <input checked="" type="checkbox"/> 一般使用者
內容摘要：	<p>1.目的</p> <p>本參考指引旨在提供有意採用 SOC(Security Operation Center)的方法，進行資安事故管理的政府機關，在規劃導入 SOC 方案時之參考。本指引屬於建議性質，政府機關(構)可參考本指引，但不以此為限，以考量機關之風險與需求，訂定符合自己需求的 SOC 導入方案。</p> <p>2.內容簡述</p> <p>本指引以事前預防、事中監看與事後處理三個階段的資安事故生命週期，提出 SOC 的資安警訊管理、資安弱點管理、資安設備管理、資安事件監看與資安事故處理五大功能架構，並建議導入時應注意的事項。</p> <p>3.文件架構</p> <p>第壹章前言，說明 SOC 的興起，相關名詞定義及適用對象。第貳章 SOC 需求，說明 SOC 的適用範圍與 SOC 的功能。並從資源投入、機關規模與機關的主觀條件分析及選擇 SOC 的解決方案。第參章，SOC 導入，說明 SOC 與 ISMS(Information Security Management System)關係，以及如何選擇建置方案，第肆章 SOC 實務參考，第伍章參考文獻。</p>
關鍵詞	資安監控中心、SOC、SOC 建置方案

目 次

1. 前言	1
1.1. SOC 的興起	1
1.2. SOC 相關名詞	1
1.3. 適用對象	5
2. SOC 需求	7
2.1. SOC 適用範圍	7
2.2. SOC 功能	7
3. SOC 導入	11
3.1. SOC 與 ISMS	11
3.2. 方案選擇分析	15
4. SOC 實務參考	36
5. 參考文獻	37
6. 附件	38
6.1. 附件 1 修訂歷史紀錄	38

圖 目 次

圖 1	SOC 架構圖	8
圖 2	SOC 資料流概念圖	10
圖 3	SOC 應變流程圖	12

表 目 次

表 1	SOC 參考指引適用對象對照表	5
表 2	資安事故作業流程對應表.....	12
表 3	資安警訊管理方式比較表.....	16
表 4	弱點掃描取得方式比較表.....	17
表 5	資安設備管理成本比較.....	18
表 6	IDS/IPS 管理能量取得方式比較.....	18
表 7	資安事件監看需求資源.....	19
表 8	資安事件監看能量取得方式成本比較表	25
表 9	SOC 功能總表	26
表 10	資安事故應變控制措施建議表	27
表 11	各級機關 SOC 導入措施實施建議	28
表 12	機關導入 SOC 自我查核表	30

1. 前言

1.1.SOC 的興起

隨著網際網路技術成熟與應用的高速發展。企業組織或是政府機關皆透過網際網路進行資料交換或是提供便利的電子化服務或網路服務。但便利的服務使用方式下也讓駭客有了可乘之機。並且網路入侵手法日新月異，導致網路資訊安全的問題不斷地遭受考驗。因此，為了保護自身重要資源，企業組織或是政府機關紛紛採購各種資安防護系統來抵禦外部攻擊。目前相關的資安技術產品如：防火牆、防毒軟體、虛擬私人網路 (VPN, Virtual Private Network)、安全掃描以及入侵偵測系統 (IDS, Intrusion Detection System)，網路應用程式防火牆(WAF, Web Application Firewall) 等，已廣泛為企業組織及政府機關運用在建置資安環境。但隨著每天數以萬計的資安事件及系統紀錄等需要被處理或管理，讓網管或資安人員難以逐一處理。同時單一的資安產品並無法提供完整的資安防護功能。故應將資安防護視為一服務流程(service process)。因此，將安全需求訂定成資安政策，並整合相關資安技術產品和緊急應變中心，而架構成的資安防護中心 (Security Operation Center, SOC)，為整體資安防護的趨勢。並且，為了防護多變且組織化的駭客攻擊，如進階持續性威脅(Advanced Persistent Threat)，利用資安防護中心協助蒐集及分析資安事件，找出有用的或是被駭客攻擊的相關資訊，來加強網路攻擊防禦，也是目前的趨勢。

1.2.SOC 相關名詞

SOC 是一個整合性資安防護管理概念，政府單位主管、資訊人員、一般使用者、資訊委外業者、SOC 建置業者以及 SOC 委外服務業者對於 SOC 的定義與解釋往往南轅北轍，本指引將就 SOC 的功能與服務作一說明。在界定何謂 SOC 之前，首先需先瞭解下列幾個 SOC 相關名詞：

- SOC(Security Operation Center)

資訊安全監控中心 SOC (Security Operation Center) 管理組織的資安產品、網路設備、使用者設備，以及系統中任何可能違反資訊安全 CIA 的內容。並提供 24*7 的服務負責監看，偵測，以及隔離資安事故。可視為資安事件監控與資安事故處理之作業中心，該中心由人員 (People)、產品 (Product) 及程序 (Procedure) 整合而來。資訊安全監控中心，必須要對所負責的組織的資安事件的監看以及資安事故的處理，以確保組織的資訊安全。通常，SOC 具備資安警訊管理、資安弱點管理、資安設備管理、資安事件監看與資安事故處理等五項基本功能[1]，通常一個 SOC 會對多個監看區域以分散收集、集中管理方式達成上述功能。

- MSS(Managed Security Service)

MSS 可視為「SOC 委外服務之通稱」，國際知名的資訊產業研究業者 Gartner 長期針對 SOC 委外服務產業進行觀察並提出研究報告，Gartner 將 MSS 定義為「An MSS includes remote, subscription-based monitoring and/or management of Firewalls, intrusion detection and prevention functions via customer-premises-based or network-based devices」，MSS 包含遠端及藉由客戶或網路設備之防火牆、入侵偵測之監看或管理之申請之防護服務。通常 MSS 以現場或遠端方式提供 7x24 的即時監看、防護、警戒提升與應變程序[2]。

- MSSP(Managed Security Service Provider)

SOC 委外服務之廠商。

- SIEM(Security Information Event Management)

資訊安全事件管理平台，Gartner 將 SIEM 定義為「Security information and event management (SIEM) technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources. It

also supports compliance reporting and incident investigation through analysis of historical data from these sources. The core capabilities of SIEM technology are a broad scope of event collection and the ability to correlate and analyze events across disparate sources. SIEM 可提供從多種資料來源中即時收集或從歷史資安事件分析而產生的威脅偵測及資安事故應變。同時也提供合適的報表以及歷史資安事故的分析。SIEM 的核心能力就是從各種不同的來源收集、關聯、以及分析資安事件。良好的 SIEM 可以讓 SOC 事倍功半，故在建制 SOC 時，亦可將 SIEM 列入評估的考量。

- 資安事件(Information Security Event)

資安事件指的是系統、服務或網路狀態可能破壞資安政策或是導致安全防護的失效，或是進入一個安全攸關的未知狀態。

- 資安事故(Information Security Incident)

資安事故指的是一起或一連串非預期的資安事件，有極高的可能危及組織營運與威脅資訊安全。

- SOC 自建

SOC 自建是指機關自行採購設備，並由 IT 部門負責 24*7 監控業務。

- SOC 委外

SOC 委外是指，SOC 業者提供監控設備，再由遠端進行資安監控事宜。

- SOC 協同維護

SOC 協同維護是指 SOC 業者與機關各負責一部分監控業務，常見的方式有分時共管，正常上班時間由機關人力執行監控，非上班時間則由 SOC 業者負責監控。

- SOC 共同供應契約

為簡化行政流程，使較小的機關能快速且方便的選擇資安監控方案，故設計 SOC 共同供應契約，讓機關可以快速且方便挑選適合自己的 SOC 服務。

- SOC RFP 範本

技服中心提供機關監控環境部屬、資安事件(故)監控、資安事件(故)通報與應變處理及資安威脅預警等四項資安服務參考。

1.3.適用對象

本參考指引提供有意採用 SOC 的方法，進行資安事故管理的政府機關，在規劃導入方案時之參考，本指引適用對象包含「一般主管」、「資訊人員」、「資安人員」及「一般使用者」，以對資安業務相關人員對 SOC 有較清楚的了解。

表1 SOC 參考指引適用對象對照表

章	節	款	一般 主管	資訊 人員	資安 人員	一般使 用者
1.前言			○	○	○	○
	1.1SOC 的興起		○	○	○	○
	1.2SOC 相關名詞		○	○	○	○
	1.3 適用對象		○	○	○	○
2.SOC 需求						
	2.1SOC 適用範圍		○	○	○	○
	2.2SOC 功能	2.2.1 資安警訊 管理				
		2.2.2 資安弱點 管理				
		2.2.3 資安設備 管理	○	○	○	△
		2.2.4 資安事件 監看				
		2.2.5 資安事故 處理				
3.SOC 導入			○	○	○	△

	3.1SOC 與 ISMS	3.1.1SOC 與 ISMS 關係 3.1.2SOC 與資安事故應變作業實務	○	○	○	△
	3.2 方案選擇分析	3.2.1SOC 解決方案說明與投入資源分析	○	○	○	△
		3.2.2SOC 解決方案選擇參考	○	○	○	△
4.SOC 實務參考			△	○	○	△
5.參考文獻			△	△	△	△
附註	各項符號代表意義說明如下： ○：詳閱；△：參考					

資料來源：本計畫整理

2. SOC 需求

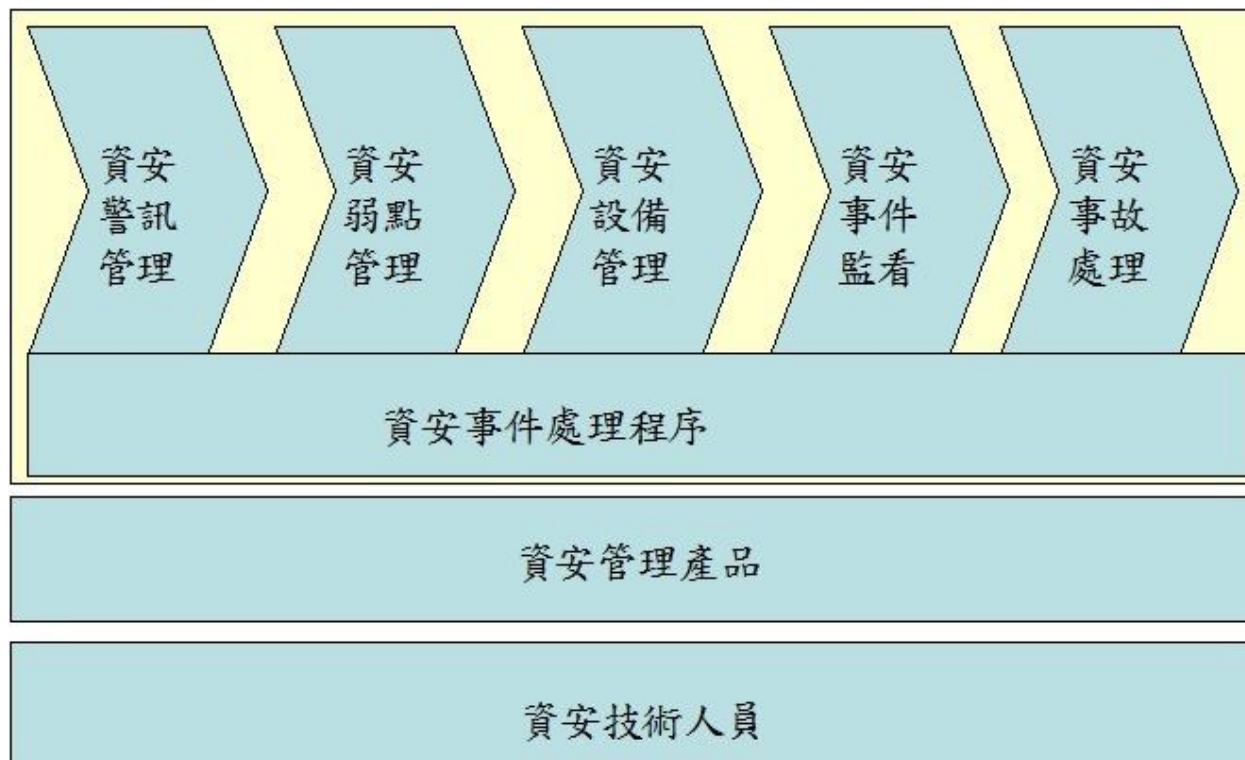
2.1.SOC 適用範圍

隨著網際網路的發展一日千里，網路應用跨入 Web 2.0 的時代，網際網路成了人人皆可參與與發展的環境，資訊的交換更快速，也更方便。無論是政府機關或民間企業，均配備員工可連接網際網路的電腦，並能自由上網，以方便人員工作時交換訊息與尋找資料。然而，在享受網際網路便利的同時，資訊安全的風險也隨之增加，資訊安全的威脅也由傳統認知的重要資訊系統安全擴散到廣大的一般使用者。在資訊安全的三大面向：機密性 (Confidentiality)、完整性(Integrity)與可用性(Availability)中，SOC 主要任務在於守護機關資訊安全的機密性，而除了重要資訊系統有機密資訊需要保護外，每位員工的個人電腦所儲存的機密資訊亦是外部有心人覬覦的珍寶。經濟學領域著名的木桶理論告訴我們，一隻木桶存水量的多少，不取決於最長的那塊木板，而取決於最短的那塊木板。因此，在考慮採用 SOC 解決方案之時，除了重要資訊系統需要涵蓋外，一般使用者端與對外服務伺服器網段(一般稱為 DMZ 非軍事區，Demilitarized Zone)也都應該是涵蓋的對象，以避免外來入侵者從 SOC 未防禦的區域進行滲透，造成資訊安全功虧一匱的情形，另外，由於 SOC 具有規模經濟的特性，涵蓋的範圍越廣，平均成本越低，因此，對有心導入的機關來說，將 SOC 防護範圍涵蓋全機關的資訊網路（甚至是有固定建立網路連線的外部單位也不應遺漏），才是導入 SOC 的最佳策略。但需了解，導入 SOC 並非就不會有安全事件發生，而是可降低資安風險。

2.2.SOC 功能

資安事故的管理，並非等到事故發生後才進行的處理作為，而應包含從事故發生前的預防、事故發生時的監看以及事故發生後的善後全程管理。參考國家資通安全會報與國內外 SOC 業者之經驗，SOC 約可分為五項主要功能，事前預防的部份包括「資安警訊管理」與「資安弱點管理」；事中監看

的部份包括「資安設備管理」與「資安事件監看」；事後處理的部份為「資安事故處理」，而這五個功能，須由資安人員、資安管理產品以及資安事件處理程序來完成，詳見圖 1 所示，以下將針對各階段功能進行說明。



資料來源：[1]

圖1 SOC 架構圖

2.2.1. 資安警訊管理

由於資訊系統的設計日益複雜，伴隨著系統設計上的弱點造成系統安全出現危機的情形也越來越頻繁，這類型的資安警訊除了在世界各國的 CERT 上會公佈之外，許多資安設備、資安服務或系統大廠也會積極蒐集這些資訊，以服務其客戶，近年來，這些警訊發布頻率日益提高，一旦未取得最新的資安警訊，將系統新發現的弱點進行修補，系統就可能毫無保護而暴露在駭客的攻擊目標下，SOC 的其中一項功能就是做資安警訊蒐集，依所蒐集之警訊判斷對於所防護之系統是否有風險，以判斷是否需做修補。

2.2.2. 資安弱點管理

縱使外在資安威脅橫行，但只要系統沒有相關的弱點存在，外在威脅也不構成風險。但是實際的情形卻永遠不會那麼理想，除了不斷的有新的弱點被發現之外，一些原始安全的設計也可能基於人性的因素被有意無意的規避。因此，弱點管理的部份也是 SOC 的功能。弱點掃描和滲透測試是比較常見的稽核方式，這些弱點管理的工作必須定期執行，同時對於被發現的弱點進行補強，方能確保系統沒有可遭利用的弱點。如此，可提升 SOC 所監看的資安事件之有效性。

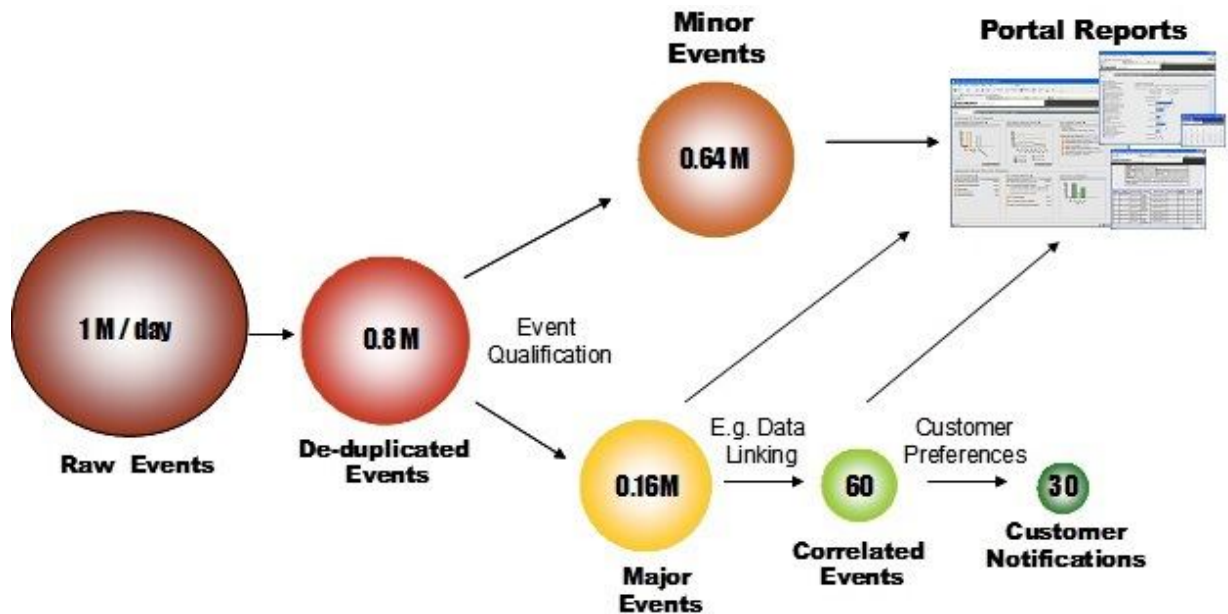
2.2.3. 資安設備管理

以目前的企業或政府機關資訊環境來看，或多或少都已經有資安設備在進行安全防護，最為人所知的就是安裝在個人電腦的防毒系統，再來就是部署於網路進出大門的防火牆，以及為了防範社交工程的危害而佈置的電子郵件檢測系統。並且為了降低機關的網站主機遭到入侵的風險，也需要佈置網路應用程式防火牆(Web Application Firewall)。而也有越來越多的機關會安裝入侵偵測系統(Intrusion Detection System, IDS)或是入侵防禦系統(Intrusion Prevention System, IPS)來針對外部網路攻擊進行防禦。然而，這些設備並不是一安裝完成後就可以高枕無憂。防毒系統若沒有定期更新病毒碼，防火牆規則設定若不定期審查，IDS 與 IPS 的 log 若不定期檢視，再多的資安設備也是形同虛設，因此，資安設備的管理，對 SOC 來說是非常重要的功能。

2.2.4. 資安事件監看

資安事件的發生是不分晝夜的，一旦系統遭入侵成功未被及時發現，駭客即可在很短的時間將衝擊蔓延或是將入侵的軌跡隱藏，屆時要再進行事故處理就很難界定傷害範圍。資安事件監看也是 SOC 最重要的價值，就是必須能 24 小時監看資安事件的發生，並在事件發生時立即處理。由於從 IDS、防火牆等資安設備回報的資安事件數量龐大，在資安事件監看上，就有賴 SOC 平台進行初步的資料過濾，再由專業的資安技術人員分析，以進行最

後的判斷，SOC 資料流的概念如圖 2 所示，將大量的資安事件資料，篩選出極少數需要注意的，可能形成事故的資訊，供監看人員分析，並同時批次將為數龐大的原始資料傳送回 SOC 進行資料倉儲，以作為後續事故處理得佐證，是 SOC 平台最重要的功能。



資料來源：本計畫整理

圖2 SOC 資料流概念圖

2.2.5. 資安事故處理

當資安事故發生後，要進行的就是資安事故的後續處理與改善，事故處理的方式可大可小，端視受害的系統重要性與關鍵性，重要性較低的個人電腦或內部伺服器，可以逕行重新安裝作業系統的方式解決，但若是重要性高的電腦或是必須保留下受駭證據的設備，就需要專業的電腦鑑識人員對受害主機進行電腦鑑識與蒐證，在這方面，SOC 記錄下來的 IDS、防火牆或防毒系統紀錄將發揮很高的作用了。

3. SOC 導入

3.1.SOC 與 ISMS

3.1.1. SOC 與 ISMS 的關係

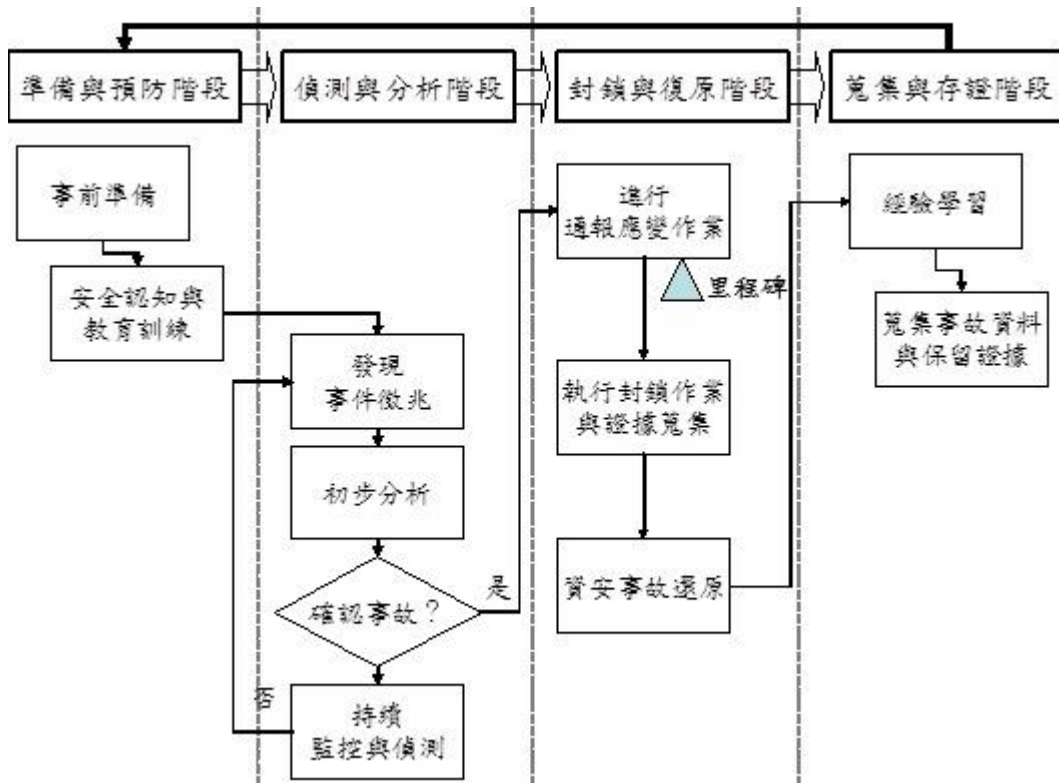
在國家資通安全會報的要求下，各級政府機關均已完成或正在進行 ISMS（資訊安全管理制度，Information Security Management System）的導入，ISO 27001:2005 資訊安全管理系統—要求事項，其控制目標與控制措施中，更將資訊安全事故管理（Information Security Incident Management）列為獨立的一個章節（A.13），可見資安事故管理在 ISMS 中的重要性。A.13 資訊安全事故管理 Information Security Incident Management 中，共有兩個控制目標與五個控制措施分述如下[3][4]：

- 通報資訊安全事件與弱點 Reporting information security events and weaknesses
- 通報資訊安全事件 Reporting information security events
- 通報安全弱點 Reporting security weaknesses
- 資訊安全事故與改進的管理 Management of information security incidents and improvement
- 責任與程序 Responsibilities and procedures
- 從資訊安全事故中學習 Learning from information security and incidents
- 證據的收集 Collection of evidence

依上述對於在 ISMS 的管理上，SOC 的功能涵蓋資訊安全事故管理的控制措施，透過 SOC 的運作，可對資安事故進行有效的安全管控，因此，導入 ISMS 與 SOC 這兩項政策在實務上是資安管理相輔相成的兩種工具。

3.1.2. SOC 與資安事故應變作業實務

在 ISO27001:2005 中，都沒有對於資安事故管理程序作一清楚的說明。故以 ISO/IEC TR 18044 為依據，資安事故應變處理流程，也可作為導入 SOC 時可參考的資安應變指引。資安事故應變處理流程詳見圖 3 所示：



資料來源：[5]

圖3 SOC 應變流程圖

現行政府機關(構)之通報應變流程，習慣以發現資安事故通報開始，執行應變作業在後，殊不知完善的事前準備工作乃為應變的成功關鍵，藉偵測與分析才得以發現資安事故，立即通報僅是應變管理程序的重要項目之一，隨後的封鎖、消除與復原才是應變工作的重點，應變之後的蒐集與存證，讓組織建置資安事故知識庫得以記取教訓，並提供經驗分享，研擬預防措施，以奠定資安防護之基石。資安事故應變作業流程對應表，詳見表 1 所示。

表2 資安事故作業流程對應表

通報應變作業	應變階段劃分	資安事故應變作業管理流程
--------	--------	--------------

通報應變作業	應變階段劃分	資安事故應變作業管理流程
事前安全防護	準備與預防階段	事故處理的準備
		資安事故的預防
事中緊急應變	偵測與分析階段	事故的徵兆
		徵兆來源警示
		資安事故的分析
		資安事故的紀錄
		資安事故處理優先順序
		通報作業
事後復原作業	封鎖與復原階段	執行封鎖策略
		證據蒐集與處理
		識別攻擊者
		根除與復原
	蒐集與存證階段	經驗學習
		蒐集事故資料
		證據保留

資料來源：本計畫整理

依行政院資通安全辦公室「國家資通安全通報應變作業綱要」提到各級政府機關(構)應建立資安事件之事前安全防護、事中緊急應變及事後復原作業機制[7]。相關作業如下：

3.1.2.1. 事前安全防護

- (1)應訂定災害預防、緊急應變程序、復原計畫等防護措施並定期演練，以建立緊急應變能量。
- (2)應規劃建置資通安全整體防護環境，對於機敏文件、資料及檔案等應採取加密或實體隔離等防護措施。

- (3)應依資通安全防護需要，執行入侵偵測、安全掃描及弱點檢測等安全檢測工作，以做好事前防禦準備。
- (4)應定期實施安全稽核、網路監控及人員安全管理等機制，以強化資通安全整體防護能力，降低安全威脅及災害損失。
- (5)應針對上述建立之資通安全防護環境及相關措施，列入年度定期稽核項目，每半年實施內部稽核乙次，以儘早發現系統安全弱點並完成修復補強。
- (6)應對機關內所建置或委外管理等資安相關紀錄定期提供資安辦。
- (7)委外管理機關(構)預於合約內，訂定承商提供相關資安紀錄。

3.1.2.2. 事中緊急應變

- (1)應就資安事件發生原因、影響等級、可能影響範圍、可能損失、是否需要支援等項目逐一檢討與處置，並保留被入侵或破壞相關證據。
- (2)查詢國家資通安全通報應變網站、系統弱點(病毒)資料庫或聯絡技術支援單位(或廠商)等方式，尋求解決方案。如無法解決，應迅速向主管機關或資安辦反應，請求提供相關技術支援。
- (3)依訂定之緊急應變計畫，實施緊急應變處置，並持續監控與追蹤管制。
- (4)視資安事件損壞程度啟動備援計畫、異地備援或備援中心等應變措施，以防止事件擴大。
- (5)評估資安事件對業務運作造成之衝擊，並進行損害管制。
- (6)資安事件如涉及刑責，應做好證據保全工作，以聯繫檢警調單位協助偵查。

3.1.2.3. 事後復原作業

- (1)在執行復原重建工作時，應執行環境重建、系統復原及掃描作業，俟系

統正常運作後即進行安全備份、資料復原等相關事宜。

- (2)在完成復原重建工作後，應將復原過程之完整紀錄(如資安事件原因分析及檢討改善方案、防止類似事件再次發生之具體方案、稽核軌跡及蒐集分析相關證據等資料)，予以建檔管制，以利爾後查考使用。
- (3)全面檢討網路安全措施、修補安全弱點、修正防火牆設定等具體改善措施，以防止類似入侵或攻擊情事再度發生，並視需要修訂應變計畫。

資安事件結束後，應彙整事件之處置過程紀錄、解決方案及強化措施等資訊，並提送「資通安全處理小組」及資安辦檢討，以強化資通安全防護機制。

3.2. 方案選擇分析

3.2.1. SOC 解決方案說明與投入資源分析

為達到事前預防、事中監看以及事後處理的資安整體防護策略，在導入 SOC 時，資安警訊管理、資安弱點管理、資安設備管理、資安事件監看與資安事故處理等五大資安防護功能均宜建立才是一個完整的 SOC。以下將對建立這五大資安防護能量的具體資源投入與取得方式進行分析。

●資安警訊管理

資安警訊的取得方式有直接訂閱服務與客製化訂閱服務兩種方式，許多資安組織、資安公司以及系統大廠都會定期公佈最新的資安警訊，有些還有提供 E-mail 通知的服務供訂閱，但這些資訊通常比較雜亂，直接訂閱時，仍需要有人花時間進行整理與篩選，才能得到所需要的資訊，有些專門進行資安警訊管理的公司，可以針對客戶的需求將客戶有需要的資訊提供給客戶，且提供深入的分析報告，此兩種服務方式比較，詳見表 3 所示。

表3 資安警訊管理方式比較表

取得方式	直接訂閱服務	客製化訂閱服務
人力資源投入	高，需進行分析篩選	低
預算資源投入	低，許多資安警訊訂閱服務為免費。	高，客製化訂閱服務費用較高。
程序建立投入	無	無

資料來源：本計畫整理

●資安弱點管理

資安弱點管理的方式較常見的有弱點掃描與滲透測試兩種，弱點掃描為透過弱點掃描軟體對網路上的機器進行已知的系統弱點或弱點進行掃描，依據掃描的結果判斷系統是否有弱點可能被駭客利用；滲透測試則是針對有侷限的範圍，在給定的時間，在受測機關同意的範圍內，由外部測試者進行各種方式的測試，測試的方式就不僅限於系統弱點，包括應用系統設計的缺失，安全管理上的疏漏都應納入滲透測試。這兩種方式各有優劣，往往在資安弱點管理上是兩者兼施以互補不足。弱點掃描可分為委外、自建與協同維運三種，此三種取得方式與投入資源比較，詳見表 4 所示；滲透測試則只有委外一途。

表4 弱點掃描取得方式比較表

取得方式	委外	自建	協同維運
預算資源投入	按服務範圍計價 (持續性支出)	1.產品教育訓練 2.報表解讀能力 建立 3.軟體取得成本 (一次性支出) 4.軟體更新費用 (持續性支出)	1.產品教育訓練 2.報表解讀能力 建立 3.軟體取得成本 (一次性支出) 4.軟體更新費用 (持續性支出) 5報表解讀諮詢費 用
程序建立投入	無	1.弱點掃瞄執行 程序 2.弱點補強程序	1.弱點掃瞄執行 程序 2.弱點補強程序

資料來源：本計畫整理

由於滲透測試需專業人力全心投入，測試方法與分析均依靠經驗，因此在成本上相對弱點掃描高出許多，在弱點管理上，弱點掃描與滲透測試往往會互相搭配執行，以茲互補。例如：每月或每季執行大範圍的弱點掃描，每半年或一年執行重要主機之滲透測試。

●資安設備管理

一般最常見的資安設備包括：防毒系統、防火牆（Firewall）、網路應用程式防火牆(Web Application Firewall)、電子郵件檢測系統以及入侵偵測/防禦系統(IDS/IPS)，這些設備使用上的專業度較高，往往有安裝完就不再更新或管理的情形，許多資安事件的發生未被及時發現，都是肇因於資安設備的管理失當以致沒有發揮該有的作用。資安設備的管理工作主要有兩個：

維護(maintain)與更新(update)。維護是確保系統的正常運作；更新則是定期更新防毒軟體的病毒碼或是入侵偵測/防禦系統的偵測碼，有關此五種主要資安設備需投入的管理成本比較，詳見表 4 所示。

表5 資安設備管理成本比較

	維護	更新
防毒系統	少	多
防火牆	少	少
網路應用程式防火牆	少	多
電子郵件檢測	少	多
入侵偵測/防禦系統	多	多

資料來源：本計畫整理

由表 4 可以看出，資安設備中需要投入管理成本最多的設備是入侵偵測/防禦系統，因此，在入侵偵測/防禦系統的維護與更新上，就有委外、自行維護與協同維運三種方案，其比較詳見表 5 所示：

表6 IDS/IPS 管理能量取得方式比較

取得方式	委外	自行維護	協同維運
人力資源投入	少	多	中
預算資源投入	委外管理費用(持續性支出)	產品教育訓練費用(一次性支出)	委外管理費用(持續性支出)
程序建立投入	無	1.系統維護程序 2.系統更新程序	1.系統維護程序 2.系統更新程序

資料來源：本計畫整理

其中委外管理費用是持續性支出，而教育訓練費用是一次性支出。

●資安事件監看

資安事件監看是 SOC 最核心的功能，人力資源、預算投入以及程序建立三方面的資源投入都高於其他幾項功能，然而，能提供即時的事件監看與處理也是 SOC 最核心的價值。為達成資安事件監看的目的必須取得的資源規格詳見表 6 所示。

表7 資安事件監看需求資源

資源類型		說明
A 人力資源	A-1 值班監看人員	執行 7 天 24 小時輪班監看，針對資安設備偵測到的資安事件進行第一線的分析與判斷。
	A-1-1 人數	必須能維持 7 天 24 小時的輪班人力，建議至少 4 人以上。
	A-1-2 工作職掌	1.即時監控資安事件 2.追蹤問題處理流程，確保問題獲得解決 3.依循過去事故處理經驗提供解決方案
	A-1-3 專業要求	1.對所使用之資安產品有基本技能 2.系統與網路管理專業知識
	A-2 系統管理人員	維護監看系統的正常運作。
	A-2-1 人數	至少 2 人
	A-2-2 工作職掌	1.修復監看系統的異常 2.對監看系統版本等內容做更新及管控
	A-2-3 專業要求	1.作業系統管理 2.網路管理 3.具備所使用資安產品之實務經驗 4.能與所使用資安產品原廠保持溝通及合作
	A-3 資深人員	值班監看人員經過第一線判斷無法自行處理時，接手執行第二線資安事故處理之工作。

資源類型	說明	
	A-3-1 人數	至少 1 人
	A-3-2 工作職掌	1.解決一線監看人員無法處理的資安事件 2.提供新的資安事故解決方案 3.設定資安工具、事件處理機制以及所需的報表
	A-3-3 專業要求	1.網路攻擊判斷 2.安全紀錄分析 3.資安事故處理 4.電腦鑑識技術
B 設備	B-1 資安設備	部署於可能遭入侵的網路或主機，以阻擋或偵測攻擊行為的發生。
	B-1-1 入侵偵測系統	部署於可能遭入侵的網路，透過定義檔的比對，偵測可疑的網路封包，並發出警訊。
	B-1-2 防火牆	部署於可能遭入侵的網路邊界，以通訊協定或連接埠為主的存取政策，控制網路流量的進出，並可記錄網路流量。
	B-1-3 防毒軟體	部署於可能遭入侵的主機，偵測並阻擋惡意程式的入侵。
	B-1-4 其他有資安紀錄檔之設備	如同伺服器主機的安全紀錄、路由器的安全紀錄、主機型入侵偵測系統等。
	B-2 SIEM(安全資訊管理工具，一般作為 SOC 平台)	能將異種資安設備的紀錄，透過網路蒐集，並能轉換為相同的格式紀錄；並有將各種紀錄資安事件，進行初步判斷，篩選出可能為資安事故的資安事件，由專業人員進行後續分析判斷。 SIEM 一般為 Client Server 架構，Client 端為

資源類型	說明
	log 資料蒐集器，接收各種資安設備的 log 輸出之 log，以下稱為 SOC agent，Server 端則為資料儲存與監看人員分析的平台，以下稱為 SOC Server。
B-2-1 日誌資料蒐集	屬於 SOC agent 的功能，整合收集網路上各項重要設備（如主機、伺服器、資安設備、網路設備、防毒系統、資產資訊、系統漏洞及弱點掃描資訊）事件訊息，透過特定的方式與傳輸格式，將其原始事件之安全日誌 (Raw Data) 主動傳輸或被動存取方式至資訊安全監控中心 (SOC) 系統。
B-2-2 紀錄檔正規化	屬於 SOC agent 的功能，正規化 (Normalization) 與過濾 (Filtering) 的處理主要將收集來的事件日誌進行「事件減量(過濾與合併重複事件)」，並把減量後的安全事件標準化、格式化後，再進行關聯分析。由於各項被監控設備所產生之原始事件日誌皆不同格式，為能進行關聯分析，將日誌加以標準化、一致性格式是需要的。
B-2-3 事故判斷規則	一般稱為 correlation rule，依據不同的產品，不一定在 agent 或 Server 端，每一筆資安設備 log 都可以算是一個資安事件，但是會形成事故的僅佔大量資安事件中的一小部份，而會形成事故的資安事件往往具有某些規則，SOC 平台必須有能力透過這些規則從大量的

資源類型	說明
	資安事件篩選出少量可能形成事故的事件，由監看人員進行分析以做最後的判斷，事故判斷規則的強弱會影響監看人員處理事件的效率與正確性，可說是 SOC 平台最舉足輕重的功能。
B-2-4 事故判斷規則輸入	由於資安事件對不同環境的影響各異，且隨著時間的改變，也會不斷有新的偵測技術與判斷規則產生，這是有賴監看人員的知識與經驗，而 SOC 平台要有一個介面給資深人員將新的事故判斷規則輸入，才能長保 SOC 可隨時掌握最新的資安攻擊型態。
B-2-5 事故問題單管理	SOC 平台判斷為資安事故的事件，必須有後續的處理紀錄與追蹤，因此要有一問題單管理系統，事故發生時開單，處理完畢後關單結案，處理過程都可以留下紀錄。資安事故必須相當謹慎，所有查詢過的資料，做過的檢查，執行的時間等都必須要留下紀錄，一則便於稽核，一則留下處理的軌跡，以供其他人員做類似事故處理的參考。
B-2-6 資安事件與事故資料庫	SOC 平台必須有龐大的資料庫以儲存經手的資安事件與事故，除了定時的監看報告產出需要外，嚴重的事件需要調閱證據時，SOC 資料庫應該也要有最完整的證據保存。
B-2-7 資安報表產生	SOC 平台必須可設定在指定時間或指定事件發生後製作報表。報表格式如 CSV、PDF 及 HTML，管理者須可將報表發佈到資安入口網

資源類型		說明
		站上。另須提供使用者可自行設計開發新報表，可依資產、IP、Port、事件紀錄類型、資訊安全事件類型、資訊安全事故等級、通訊協定等條件產生自訂報表。
C 流程	C-1 資安事故處理流程	為確保每一個監看人員處理事件的品質一致，在 SOC 維運時，建立一套資安事故處理流程是必要的，問題單開出時，有哪些資料一定要查詢的，有哪些地方一定要檢查，如何與受攻擊端的人員互動，如何進行後續的處理，何種情況可以結案，依據不同的環境可以有不同的處理流程，一套固定的處理流程是有必要的。
	C-2 通報應變流程	若有資安事故發生，必須要向上通報，最終都要通報到(國家資通安全會報，但是中間的流程則要明確訂定，是先通報主管機關在通報會報，或是統一由主管機關通報，這些細節都必須明確訂定。

資料來源：本計畫整理

在監看能量的取得上，有委外、自建與協同維運三種模式，委外即是將監看作業的服務委託給外界的 MSSP，利用 MSSP 的 SOC 設備與人員，提供遠端的資安事件監看服務；而自建即是自行購置一套 SOC 平台與訓練自己既有的人員，自建一個內部的 SOC，監看自己環境的資安事件，包含：系統平台建置、持續性的 SOC 環境參數調適、營運操作與組織教育訓練、輔導建立營運流程及規範。；協同維運則是委外與自建兩種方案的結合，在建置期自行購置一套 SOC 平台，而後續的維運則由機關人員與委外廠

商協同執行，三種方案的取得上，都有人力、設備與流程建置的考量，有關委外、自建與協同維運 SOC 的成本比較詳見表 7 所示。

表8 資安事件監看能量取得方式成本比較表

取得方式	委外	自建	協同維運
人力資源投入	少，至少 1 人，執行委外管理與聯絡窗口。	多，至少 6 人，執行 7 天 24 小時輪班監控作業。	中，介於 2~6 人之間，與委外廠商共同合作執行 7 天 24 小時輪班。
地點與設備	監控平台與軟體設備均由 SOC 廠商提供。	監控平台位於機關本身，設備與軟體財產屬於機關。	主監控平台位於機關，廠商 SOC 平台協助監控。
監控模式	廠商遠端監控	直接監控	<p>模式可選：</p> <ul style="list-style-type: none"> ▪ 主平台 7 天 24 小時監控，廠商僅微駐點人力協助處理資安事件。 ▪ 主平台 5 天 8 小時監控，剩餘時間轉由廠商平台監控。
預算資源投入	委外費用(持續性支出)	<p>產品購買費用(一次性支出)</p> <p>人員訓練費用(持續性支出)</p> <p>產品維護費用(持續性支出)</p>	<p>產品購買費用(一次性支出)</p> <p>產品維護費用(持續性支出)</p> <p>委外費用(持續性支出)</p>
程序建立投入	C-2 通報應變流程	C-1 資安事故處理	C-1 資安事故處理

取得方式	委外	自建	協同維運
		流程 C-2 通報應變流程	流程 C-2 通報應變流程

資料來源：本計畫整理

●資安事故處理

資安事故的處理，基本上可以參考「國家資通安全通報應變作業綱要」，並納入 ISO 27001 A.13.資訊安全事故管理的要求，以 PDCA 持續改善流程，建立良善的資安事故管理機制。

依據以上五種對於 SOC 的功能說明，彙整本指引提到的導入 SOC 應執行的工作，以供機關參考，詳見表 9。

表9 SOC 功能總表

功能	執行工作
資安警訊管理	警訊訂閱
資安弱點管理	1.弱點掃描 2.滲透測試
資安設備管理	1.資安設備維護 2.資安設備更新
資安事件監看	1.SOC 維運人力資源 2.取得資訊與資安防護設備紀錄 3.資安監控平台與設備
資安事故處理	1.資安事故處理流程 2.通報應變流程

資料來源：本計畫整理

3.2.2. SOC 解決方案選擇參考

美國 NIST 於 2005 年 2 月公佈了 NIST Special Publication 800-53，針對美國聯邦政府資訊系統的安全防護與控制措施，區分為高、中、低風險並提出控制措施實施的建議。而關於資安事件監看與事故處理的部份定義，經參考 NIST SP 800-53 及技服中心經驗訂出資安事故應變控制措施建議表，詳見表 9 所示[6]。

表10 資安事故應變控制措施建議表

編號	控制項目	風險等級		
		低	中	高
IR-1	資安事故應變政策與程序	✓	✓	✓
IR-2	資安事故應變訓練		✓	✓
IR-3	資安事故應變測試		✓	✓
IR-4	資安事故處理	✓	✓	✓
IR-5	資安事故監看		✓	✓
IR-6	資安事故通報	✓	✓	✓
IR-7	資安事故應變協助	✓	✓	✓
IR-8	資安事故應變計畫	✓	✓	✓

資料來源：本計畫整理

國家資通安全會報將我國政府機關劃分為 A、B、C、D 四個等級，以區分各機關之風險等級。若將低風險對應至 C、D 級機關，中風險對應至 B 級機關，高風險對應至 A 級機關。以下將針對各等級之機關，依本指引列舉之 SOC 導入措施提出實施建議，詳見表 10 所示。

表11 各級機關 SOC 導入措施實施建議

項目	NIST 編號	SOC 功能	機關等級		
			C、D	B	A
0-1	IR-1	資安事故應變政策與程序	✓	✓	✓
0-2	IR-8	資安事故應變計畫	✓	✓	✓
1 資安警訊管理					
1-1	IR-2	取得最新資安警訊		✓	✓
2 資安弱點管理					
2-1	IR-3	弱點掃描		✓	✓
2-2	IR-3	滲透測試		✓	✓
3 資安設備管理					
3-1	IR-4	防毒系統	✓	✓	✓
3-2	IR-4	防火牆系統	✓	✓	✓
3-3	IR-4	網路應用程式防火牆		✓	✓
3-4	IR-4	電子郵件檢測系統		✓	✓
3-3	IR-5	入侵偵測/防禦系統		✓	✓
4 資安事件監看					

項目	NIST 編號	SOC 功能	機關等級		
			C、D	B	A
4-1	IR-5	建立 SOC 服務能量		✓	✓
5 資安事故處理					
5-1	IR-4	資安事故處理流程		✓	✓
5-2	IR-6	通報應變流程	✓	✓	✓

資料來源：本計畫整理

上表僅依資安等級區分哪些 SOC 項目應該實施，而採用何種方案實施應該是各機關最頭痛的問題，選擇自建或委外或協同維運，其中的投入資源亦有不同的考量，此時往往造成機關難以下決定，因此在做決策之前，各機關不妨依我們建議的導入 SOC 自我查核表，先對自身狀況作一總評估，再決定何種方案較適合該機關。

自我查核表包含維持 SOC 監控服務能量所需的四個面向，包括(1)監控中心實體環境(2)人力資源(3)資安服務系統(4)維運制度。每個面向以提供 SOC 服務所需資源的必要性，給予相對的加權比重。在(1)監控中心實體環境面向，我們認為此項為自建或委外最大的關鍵因素，因為選擇 SOC 自建方案，實體環境為此方案的必備要素，因此倘若機關無法提供監控中心實體環境，則建議直接委外。再者若機關雖然具備監控中心實體環境，但亦不能斷然決定自建或委外時，我們建議從(2)(3)(4)面向評估分數來考慮 SOC 建置方案。

在建置 SOC 服務所需資源中，我們認為監看的專業人才非常重要，倘若機關缺乏這方面的專才，自建 SOC 的可能性較為艱難，空有環境與軟硬體亦難展現 SOC 功能價值，因此在加權比重上，我們建議以 50% 來突顯它的不可或缺，當然其他的面向亦相對重要，在加權比重上亦有展現。

因此(2)(3)(4)項評估加總，自評分數總分低於 60 分者建議委外，80 分以上者建議自建。介於 60~80 分者建議協同維運。機關導入 SOC 自我查核表，詳見表 11。

表12 機關導入 SOC 自我查核表

SOC 項目	項目內容	建置標準	配分	自評分數
監控中心實體環境	實體機房設備	有	/	
	資安防護監控室	有		
人力資源	一線監控人員	7(人)	60	

SOC 項目	項目內容	建置標準	配分	自評分數
	二線處理人員	2(人)	20	
	三線管理人員	1(人)	20	
小計	加權		50%	
資安服務與系統	資安防護設備佈置	有	30	
	資安入口網站	有	10	
	資產管理系統	有	10	
	資安知識資料庫	有	10	
	資安事件關聯分析系統	有	10	
	報表系統	有	10	
	弱點掃描	有	10	
	滲透測試	有	10	
小計	加權		20%	
維運制度	資安設備管理程序	有	10	
	資安事件處理程序	有	10	
	資安事件監控程序	有	10	
	資安事故通報程序	有	10	
	ISO27001	有	20	
	ISO20000	有	20	
	營運持續計畫(BCP)	有	10	
	災害復原程序(DRP)	有	10	
小計	加權		30%	

資料來源：本計畫整理

項目說明：

● 監控中心環境

自建 SOC 必須具備足夠且符合實體安全相關法規的空間，來容納資安監控設備與資安監控人員，或者已經有足夠量的資安監控設備，才需要有 SOC 來做統合處理。

－ 機房設備

符合實體安全法規(如消防、門禁、實體環境安全)的機房空間與資訊安全監控設備。

－ 資安防護監控室

提供監控座位、操作空間、硬體設備給資安監控人員使用。

● 人力資源

資安監控中心所需人力資源，以及所需具備之專業技能證照。

－ 一線值班人員：負責資安監控作業、事件分析及事件通報等。

一線值班人員所需能力參考標準為具有下列證照或是同等能力如：CCNA(CISCO 網路設備認證)、CEH(駭客攻防認證)。

－ 二線處理人員：負責事件追蹤、事件處理及協助系統管理等。

二線處理人員所需能力參考標準為具有下列證照或是同等能力如：MCSE(微軟認證系統工程師)、RHCE(Linux 認證訓練)。

－ 三線管理人員：負責監督管理資安監控中心運作、以及緊急處理資安重大意外。

三線管理人員所需能力參考標準為具有下列證照或是同等能力如：ECSA(資安分析專家認證)、CISSP(資安系統專家認證)。

●資安服務與系統

資安監控中心所需具備的功能與管控的設備。

－ 資安防護設備佈置

資安基礎建設備、如 IPS、IDS、防火牆、防毒監控系統、網路安全閘道器、網路應用程式防火牆、電子郵件檢測等資安防護設備。

－ 資安入口網站

須可將關聯分析後之訊息或事件處理狀態，透過網頁儀表板或資安入口網站機制提供監控人員管理或查詢。

－ 資產管理系統

紀錄、管理電腦及網路設備資產。

－ 資安知識庫系統

記錄病毒、惡意程式等攻擊手法以及資安弱點等內容。

－ 資安事件關聯分析系統

將來自不同監控設備之系統資訊與安全事件集中到單一的管理平台，進行事件的集中儲存、比對及分析。

－ 報表系統

須可設定在指定時間或指定事件發生後製作報表。

－ 弱點掃描

檢查網站或網頁或資訊系統是否有弱點可供駭客利用攻擊。

– 滲透測試

以駭客的角度，由外部對目標網路環境作深入的安全探測，並預先找出機關資訊安全上脆弱的環節。

● 維運制度

為確保服務品質與不斷提升服務能量，資安監控中心必須有各項管理規範與事件處理程序。

– 資安設備管理程序

維護資安設備與 SIEM 平台運作正常，提供各種特徵碼、知識庫等更新服務、設備管理、組態變更管理、服務狀態監控以確保資安防護維持在最佳防禦狀態、並即時掌握服務提供狀態。

– 資安事件監控程序

即時監看資安監控平台所收集的資安事件，以及判斷是否可能形成資安事故。

– 資安事故通報程序

在資安事故發生後，迅速且即時通知負責處理的人。

– 資安事故處理程序

當資安事故發生後，進行管控動作，解除資安事故發生的原因，避免再次駭客利用相同手法入侵。

– ISO27001

確立在政策、組織、執行層面上的安全保障規劃（ISMS）均可應付潛在風險，保障必要之營運系統。

– ISO20000

確立各種資訊維運流程符合標準，能夠保障營運系統一定的服務品質。

– BCP(Business Continuity Planning):營運持續計畫

必須瞭解組織所面臨的風險發生之可能性與衝擊，能夠鑑別出影響組織成敗的重要業務，以及維運這些重要業務時所需要的資產，包括：人員、軟硬體、行政資源、通訊資源等等。根據風險評鑑的結果發展營運持續策略，以決定營運持續的整體作法。

– DRP(Disaster Response Planning):災害復原程序

可針對不同之災害復原用資源項目進行回復規劃。例如可針對資訊應用系統、資訊機房、資料庫與通訊網路服務訂定相關回復作業流程與步驟，而這些作業流程與步驟建議以標準作業流程(SOP)方式呈現。

4. SOC 實務參考

不論是採用何種方式建立 SOC 能量，對機關來說都是一筆不小的投資，而且資安專案通常敏感性較高，因此技服中心在需求規格與專案管理上提供 RFP 範本以及共同供應契約，以供機關撰寫 RFP 時參考。

5. 參考文獻

- [1] Service Management Strategies, Building Information Security Operation Center, Meta Group, 2001
- [2] Guidelines for Choosing to Outsource Security management, Gartner research, 2003
- [3] ISO/IEC 27001 Information technology – security techniques – information security management systems – requirements, International Standard Organization, 2005
- [4] 經濟部標準檢驗局，CNS27001 資訊技術-安全技術-資訊安全管理系統-要求事項，96 年 6 月
- [5] ISO/IEC TR 18044 Information technology – security techniques – information security incident management, International Standard Organization, 2004
- [6] NIST，NIST Special Publication 800-53，2005
- [7] 行政院資通安全辦公室，國家資通安全通報應變作業綱要，101 年 8 月

6. 附件

6.1.附件 1 修訂歷史紀錄

附件 1 修訂歷史紀錄

版次	修訂日期	修訂說明
V2.0	102.7.1	修訂 1.3 適用對象 之表 1 SOC 參考指引適用對象對照表，調整人員分類與適用建議。
		2.2.3 資安設備管理，新增應用程式防火牆與電子郵件檢測系統之說明，以及相對應的內容。
		刪除原第三章之 SOC 與資安事件應變作業參考指引(草案)，增訂 3.1.2 SOC 與資安事故應變作業實務章節，將資通安全通報應變作業綱要之要求納入。
		修訂 3.2.1 SOC 解決方案說明與投入資源分析。
		表 4 資安設備管理成本比較表，新增網路應用程式防火牆與電子郵件檢測系統之比較。
		修訂 3.2.2 SOC 解決方案選擇參考。
		表 10 各級機關 SOC 導入措施實施建議，新增各級機關對於網路應用程式防火牆與電子郵件檢測系統之實施建議。
		修訂 表 11 機關導入 SOC 自我查核表之評核項目與計算方式。
		修訂 4.SOC 實務參考，刪除原章節針對 RFP 要求的建議，改以導引參考另一文件 SOC RFP 範本之說明。

資料來源：本計畫整理