標準新訊

與時俱進之資訊安全管理系統標準－ISO 27001

科技與網際網路的快速進步，組織與個人藉助各類資通訊產品及工具享有便捷業務宣傳與溝通往來的同時，所面臨的資訊安全(常簡稱為資安)的威脅卻也如影隨形日益嚴峻，勒索攻擊、惡意連結、駭客入侵等資安事件屢見不鮮。隨著全球開始進入大數據與人工智慧的時代，各種通訊工具之功能更以前所未見的速度大幅精進，資訊安全必然是組織經營中不可忽視的重要環節，且資安問題不僅限於大型組織，許多中小組織亦可能成為攻擊目標，一旦疏忽資安問題導致組織內部資料或組織之利害相關者(interested parties)相關資訊外洩，將造成對組織嚴重影響與衝擊，故完善的資訊安全管理對組織長遠發展與健全營運的重要性不言可喻。有鑑於此，國際標準化組織(ISO)於去(2022)年 10 月與國際電工委員會(IEC)聯合修訂公布第三版 ISO/IEC 27001:2022「資訊安全、網宇安全和隱私保護—資訊安全管理系統—要求事項

(Information security, cybersecurity and privacy protection — Information security management systems — Requirements)」， 此一資訊安全管理系統 (Information Security Management System, ISMS) 標準之修正旨在協助組織藉由運用風險管理過程，保有相關資訊之機密性、完整性(integrity)及可用性(availability)，藉由組織本身適切的風險管理運作，使其利害相關者具有信心，從而使組織受益。

ISO/IEC 27001 為目前國際上使用最廣泛且最完整的一套檢驗資訊安全管理系統規範，可廣泛地用以保護組織之敏感性資訊，以免其發生使用不當、未經授權的存取、中斷或毀損等狀況。ISO/IEC 27001 適用於所有組織，無論其類型、規模或性質如何，並且可由內部及外部各方使用，以建立、實作、維護及持續改善資訊安全管理系統之要求事項，俾利協助組織應對資安挑戰，進一步增強其網路彈性並實施網路威脅緩解措施。所謂網路彈性係指組織在面對網路攻擊或其他網路事件時的運作能力，涉及組織採取必要的技術和措施來檢測、因應此類

事件並從中恢復、適應和學習，以提高未來彈性應變的能力。ISO 指出使用該標準可使組織得到之益處如下:

一、 保護所有形式的資訊，包括紙本的(paper-based)、雲端的(cloud-based)和數位的資料

二、 提高對網路攻擊的彈性應變能力

三、 提供一個集中管理的框架(centrally managed framework)，將所有資訊保護在一個地方

四、 確保組織範圍內(organization-wide)的保護，其中包括針對基於技術的(technology-based)風險和其他威脅

五、 應對不斷變化的安全威脅

六、 減少無效防禦技術的成本和支出

七、 保護資訊的完整性、機密性和可用性

經檢視 ISO/IEC 27001:2022，我們可以發現該標準之附錄 A「資訊安全控制措施參引」(Information security controls reference)是本次新版修訂的重要部分，該附錄簡化了控制措施架構，將上一版標準原有的 14 個安全控制節次(control clause)，調整為組織控制、人員控制、實體(Physical)控制、技術控制等四大面向(themes)之控制措施，

而控制措施項目則新增雲端服務、個人隱私等相關項目，並將不合時宜之內容予以刪併，整體控制措施項目從 114 項精實為 93 項，經查該標準中之表 A.1 所列之各項資訊安全控制措施，乃直接取自 ISO/IEC 27002:2022「資訊安全、網宇安全及隱私保護 - 資訊安全控制措施 (Information security, cybersecurity and privacy protection—Information security controls)」之第 5 節至第 8 節，且於 ISO/IEC 27001 內文之 6.1.3 節「資訊安全風險處理」一起使用。

上述 ISO/IEC 27001 之 6.1.3 節「資訊安全風險處理」控制措施的參考標準 ISO/IEC 27002，係資訊安全管理系統的實務指引文件，亦於去年修訂公布第三版，經檢視新版本之 ISO/IEC 27002 引入了五種屬性(Attributes)標籤，包括「控制措施型式」(Control type)，其屬性值由預防、偵測、改正組成；「資訊安全性質」(Information security properties)，其屬性值由機密性、完整性、可用性組成；「網宇安全概念」(Cybersecurity concepts)，其屬性值由識別、防護、偵測、因應(Respond)、回復(Recover)組成；「運作

能力」(Operational capabilities) ，其屬性值由治理(Governance)、資產管理、資訊保護、人力資源安全(Human_resource_security)、實體安全等 15 項組成；以及「安全領域」(Security domains)，其屬性值由治理與生態系統(Governance_and_Ecosystem)、保護、防禦(Defence)、彈性(Resilience)組成。ISO/IEC 27001 與 ISO/IEC 27002 標準本次修訂重點為加入隱私及個人可識別資訊的保護，使個資保護成為資訊安全管理系統之重要一環，俾能更符合現今的資訊安全管理需求。

關於 ISO/IEC 27001 的內容，除了前言、簡介、適用範圍、術語和定義外，還包括如下內容(對應 ISO/IEC 27001 的節次):

4 組織全景

4.1 瞭解組織及其全景

4.2 瞭解利害相關者之需要及期望

4.3 決定資訊安全管理系統之範圍

4.4 資訊安全管理系統

5 領導作為

5.1　領導及承諾

5.2　政策

5.3　組織角色、責任及權限

6　規劃

6.1　因應風險及機會之行動

6.2　資訊安全目標及其達成之規劃

6.3　變更之規劃

7　支援

7.1　資源

7.2　能力

7.3　認知

7.4　溝通或傳達

7.5　文件化資訊

8　運作

8.1　運作之規劃及控制

8.2　資訊安全風險評鑑

8.3　資訊安全風險處理

9　績效評估

9.1　監督、量測、分析及評估

9.2 內部稽核

9.3 管理審查

10 改善

10.1 持續改善

10.2 不符合事項及矯正措施

附錄 A 參考資訊安全控制措施

名詞對照

參考資料

資安事件代價高昂，具有破壞性，對企業、政府和社會的威脅與日俱增，故需系統化作法加以建立有效之資訊安全管理系統，對於技術系統、團隊、組織文化和日常營運都是不可或缺的。為幫助組織建立網路彈性，資訊安全管理系統能有系統地分析和管理資訊系統，其為一套政策、程序、流程和架構，若運作得宜，將可有效避免網路攻擊、資料洩露或竊取所造成的資料損失風險。為積極支持我國資訊安全領域之運作，本局 112 年 1 月 30 日已參考 ISO/IEC 27001 與 ISO/IEC 27002 國際標準調和制定 CNS 27001「資訊安全、網宇安全及隱私保

護 - 資訊安全管理系統 - 要求事項」及 CNS 27002「資訊安全、網宇安全及隱私保護 - 資訊安全控制措施」，提供組織與個人可資參據依循的資安規範，俾利各組織在資安方面能有更強的防禦力，穩固組織永續發展之目標。

上述 ISO 相關資訊另可參考 ISO 官網，本局已和 ISO 簽有授權合約，民眾只需支付權利金，即可合法取得即時並已制定公布的標準資料，歡迎各界多加利用。如需查詢本局外國標準館藏狀況、價格及購買方式，請至本局「標準資料查詢系統」查詢或撥打服務專線 02-23431980 洽詢。此外，CNS 國家標準相關資訊皆置放於本局「國家標準(CNS)網路服務系統」，歡迎各界上網免費查詢預覽，如需查詢購買方式、價格或網路操作，請撥打服務專線 02-23431994 洽詢。

參考資料來源:ISO News、ISO/IEC 27001:2022、ISO/IEC 27002:2022