

資訊安全風險管理

現代化企業大量運用IT系統，為了維護公司治理與降低營運風險，企業必需發展完整資訊安全措施，保護公司重要資訊資產，以追求永續經營的目的。面對新興科技與商業模式轉變，帶來的新型態犯罪的挑戰，中鼎堅持保護客戶的重要智慧資產，強化專案執行可靠與品質，以提升客戶信賴。並且符合業主要求或法令規定，如營業秘密法、個人資料保護法、資通安全管理法等。

資訊安全治理制度

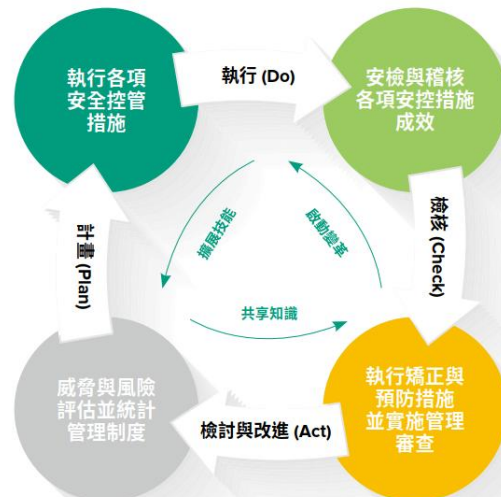
中鼎為因應各類資安威脅，於2014年起正式透過導入ISO 27001的標準進行風險管理，致力於降低風險發生的機率與影響，提升公司持續營運能力。成立資訊安全推動委員會專責組織，由總經理擔任主席(兼任資安長)，每年定期召開，負責資訊安全政策推動事宜。



資訊安全推動委員會

中鼎了解在資安風險的管理作業上，是需要以PDCA的做法不斷精進。藉由資安管理的推動與落實，以支持集團內各項業務的永續經營與發展，也是打造新世紀中鼎IT的重要基石。

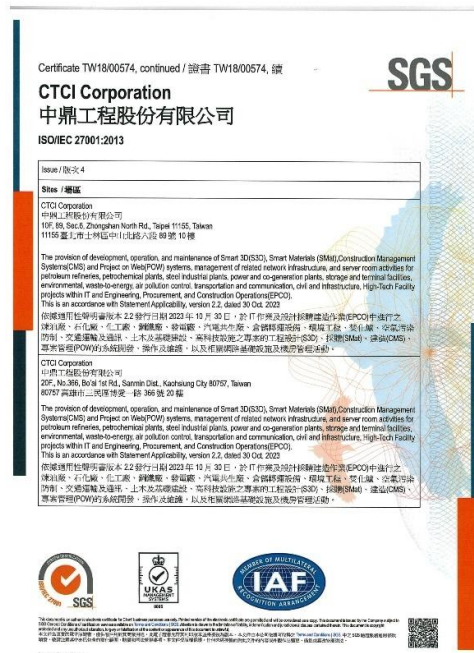
■ CTCI 的 ISMS 實施循環 - 資訊安全系統之管理循環



資訊安全管理機制

透過每年的風險評鑑作業，從各項可能的威脅與弱點組合中，分析出主要的項目包括：

- 1 詐騙集團利用偽冒的電子郵件，誘騙企業員工匯款或交易。
- 1 商業間諜或競爭對手運用駭客技術，持續滲透內部主機，竊取企業內部資料。
- 1 犯罪集團結合駭客，透過電子郵件、簡訊、社群軟體、通訊軟體，散佈具有惡意連結的內容，使受害電腦資料被加密綁架，要求付出高額贖金。
- 1 駭客透過網路發動大規模數量的連線要求，阻斷公司正常網路的運作。
- 1 內部員工使用非法軟體或將公司機敏資料複製到隨身儲存裝置，因遺失、遭竊或販賣，致使資料外洩。
- 1 天災人禍造成資訊軟硬體或受到損害，導致服務中斷或資料遺失。



持續維持ISO 27001資安管理證書有效性 (證書有效期至2025/10/31)

針對以上的風險項目，中鼎運用資安管理準則、導入科技解決方案與強化資安教育訓練，多管齊下做好資訊安全的管理機制，包括以下重點措施：

- | 定期執行內外部稽核，通過並維持ISO 27001認證，精進資安管理體系運作。
- | 持續進行社交工程攻擊模擬演練，並提供資安教育訓練，提升員工對於郵件防護意識。
- | 用戶端安裝防毒與監管軟體，封鎖USB儲存裝置的連接與自行安裝軟體的權限。另提供個人雲服務備份重要資料。
- | 針對網路層，中鼎導入中華電信資安雲的服務，結合防火牆，針對網路的流量與應用進行管制。發展內網防護與資料庫存取安全監控管理機制。
- | 透過機敏文件管控系統與磁碟加密技術，保護文件機密性。
- | 運用郵件過濾及郵件稽核系統，降低電子郵件使用的風險。
- | 導入人臉辨識於閘門管理，兼顧防疫與實體安全需求。
- | 導入外部專家執行資安健診作業，透過整合各項資訊安全項目的檢視服務，以找出整體架構的資安潛在風險，並加強防護。
- | 主機集中管理，建立機房環控與告警機制，定期執行資料備份，並每年執行災難備援演練。

資訊安全所投入之資源

中鼎每年持續投入資源於資訊安全事務，包含強化資安防禦設備、改善資安管理制度與教育訓練等，從管理面到技術面整體落實，增進資訊安全能力。對於事件的預防，除了每年在高雄備援機房執行資訊層面的企業持續營運演練外，針對重要系統資料，每週執行異地備份、保管與測試，以及每年兩次的弱點掃描，皆納入資安例行作業中。

在資安意識的提升方面，每季進行社交工程攻擊演練，針對同仁隨機抽樣，2024年共計抽選7,340人次參與演練。另針對集團創研中心與資訊部的系統管理同仁，也全面實施資安相關的教育訓練。全公司各項資安相關訓練參與總時數達到2,740小時，課程包括：辨識社交工程攻擊及資安重點宣導、ISO 27001資安事件通報、處理及調查與數位鑑識實務、ISO 27001資訊資產清單與風險評鑑作業實作指引、資訊安全通識課程等。另透過企業內部入口網站，張貼資安相關議題公告，對公司全體同仁宣導防範勒索病毒、認識電子郵件的使用安全等，共計13,386人次閱讀。

資訊安全事件

2025年度迄今無任何重大資安事故發生。