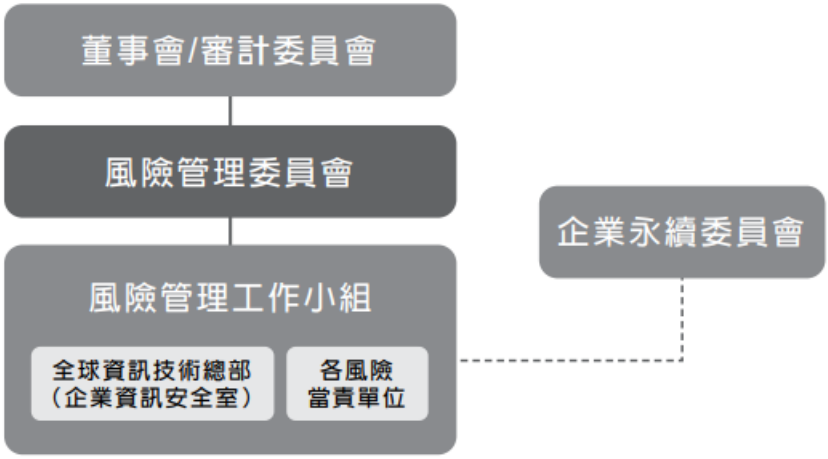
資通安全管理之資訊揭露

資通安全風險管理架構

本公司於民國 111 年設立「風險管理委員會」，全球資訊技術總部為其下轄單位之一，本公司之資訊安全及保護相關政策制定、執行、風險管理等，係由全球資訊技術總部中之企業資訊安全室負責統籌。風險管理委員會最高主管每年至少一次向董事會及審計委員會彙報資安管理成效、資安相關議題及方向。

民國 111 年 11 月 3 日向董事會及審計委員會報告-風險管理落實進度與「2022 Acer Global Security Re-architect Update」專題



資通安全政策與具體管理方案

1. 企業資訊安全管理策略與架構

企業資訊安全組織為有效落實資安管理，每 2 週開 ISMS(Information Security Management System, ISMS) 例行會議，依據規畫、執行、查核與行動（Plan-DoCheck-Act, PDCA）的管理循環機制，檢視資訊安全政策適用性與保護措施，並每年透過內部與外部稽核，確保執行狀況符合規範，維護重要資產的機密性、完整性及可用性。ISMS 著重資安風險管理，並建立基礎架構與核心系統持續通過國際資安管理系統認證 ISO/IEC 27001，從系統面、技術面、程序面降低企業資安威脅，建立符合客戶需求的機密資訊保護服務。

除 ISMS 制度外，於民國 110 年參考 NIST Cybersecurity Framework (CSF) 資安框架，加強多層資安防護， 涵蓋資安的五大面向，包括識別(建立組織規則以管理系統、人員、資產、資料和功能的網路安全風險)、保護 (建立和實施適當的安全措施以確保重要服務的運行)、偵測 (制定並實施適當的作為以識別網路安全事件的發生)、回應 (對偵測到的網路安全事件，規劃並實施適當的行動)與復原(制定並實施適當的措施以修復因網路安全事件受損的功能和服務)，落實網路安全生命週期的風險管理，逐步導入資安防禦創新技術，將資安控管機制整合入軟硬體維運、及平日作業流程，系統化監控資訊安全，利用 NIST CSF 框架來持續評估公司資安成熟度，做為未來強化的方向依據。

2. 企業資訊安全風險管理與持續改善架構

3. 具體管理方案

● 多層資安防護

裝置安全	• 全面導入端點防護 EDR (Endpoint Detection and Response) • 端點防毒措施強化惡意軟體偵測
帳號安全	• 全面導入MFA (Multi-factor authentication) 於員工在外使用公司資源，包含VPN與雲端服務 • 與第三方合作，搜索暴露在暗網的帳號，主動變更密碼
網路安全	• 強化網路防火牆與ACL (Access-control list)控管 • 導入網路存取控制措施 NAC (Network Access Control)，禁止不合規設備存取公司資源
應用程式安全	• 每年執行對外提供服務的網頁安全檢測並修正弱點 • 盤點過時及有風險的軟體套件，執行必要的升級

● 資安成效控管

公司持續透過第三方評核，回應資安風險，並予以矯正，確保資安防護機制符合產業標準。

資安成熟度評鑑	• 委託外部專家執行公司網路與資訊安全評鑑

產業標準為 Industry Avg.， 分數約為 84，成熟度為 B。

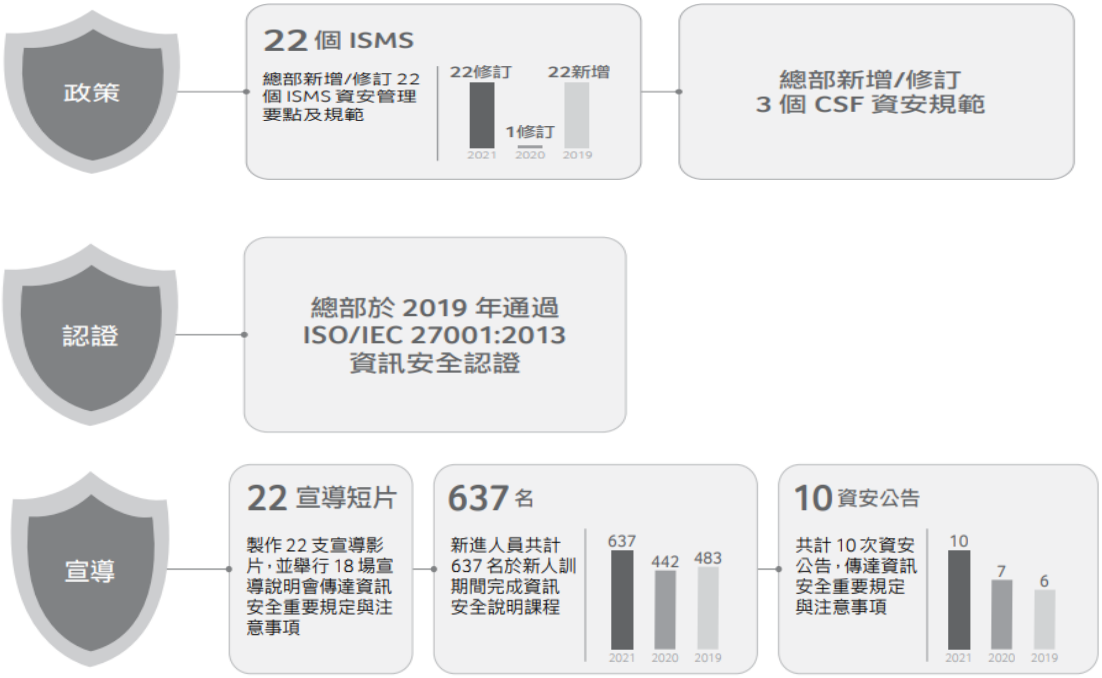
Acer 為 Acer Grade，除了因為民國 110 年 3 月全球資安事件及 10 月因印度與台灣服務網站資安事件，影響資安成熟度被扣分，其餘均保持向上趨勢，與國際產業標準對齊。

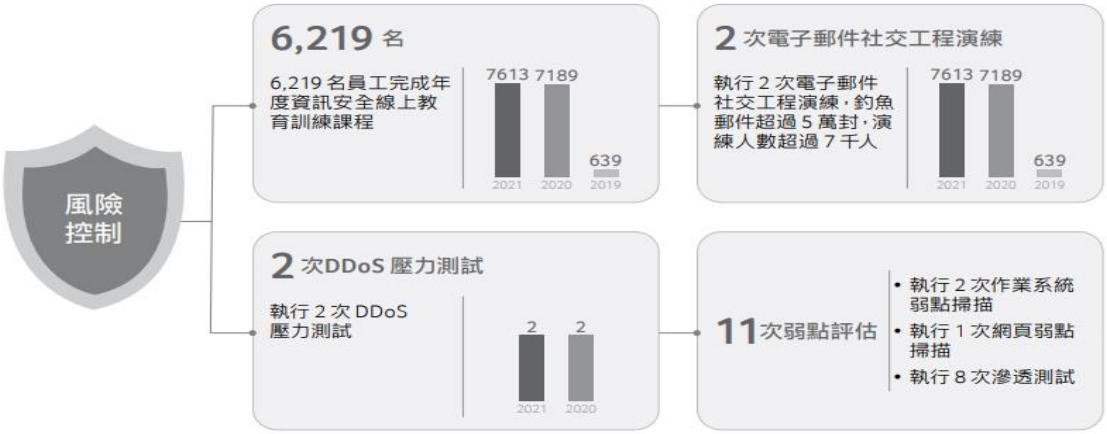
檢討與持續改善

教育訓練與宣導	• 定期舉辦教育訓練提升員工資安意識 • 加強員工對釣魚郵件攻擊的警覺性，執行釣魚郵件防禦偵測

4. 具體管理方案

民國 110 年企業資訊安全措施推動執行成果





民國 111 年資安管理強化重點：

- 重新驗證並持續維運 ISO 27001 資訊安全管理系統，落實 PDCA 持續精進管理精神，並確保資安具體落實在日常工作中。
- 擴大 ISO27001 的管理規範與認證至海外其他分公司，提升全球資安防禦水準，擴大整體安全管理之基礎以提昇公司形象及達到永續經營目標。
- 透過多樣化資安訓練活動持續增進員工整體安全意識，以提升人員資安管理能力。
- 持續落實資安情境演練，強化員工資安事件處理應變能力及公司對攻擊的風險承載度

第三方驗證紀錄：

- 2021/11/24 通過第三方資訊安全驗證公司 BSI 後續拜訪驗證宏碁公司 ISO27001: 2013 持續有效
- 2022/04/27 通過第三方資訊安全驗證公司 BSI 後續拜訪驗證宏碁公司 ISO27001: 2013 持續有效
- 2022/09/13 通過第三方資訊安全驗證公司 BSI 重新驗證宏碁公司 ISO27001: 2013 持續有效