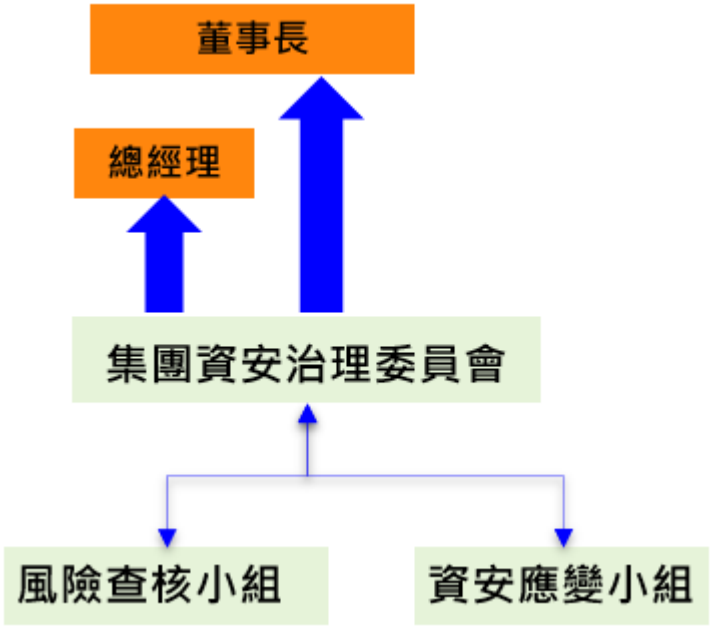
# 資通安全管理之資訊揭露

## 資通安全風險管理架構

宏碁公司於民國111年設立「風險管理執行委員會」，資安長為委員會成員之一，負責本公司之資訊安全及保護相關政策制定、執行與風險管理等，範圍包含 IT 系統 和產品資訊安全。

為進一步提升集團資訊安全風險管理，宏碁公司於民國112年設立「集團資安治理委員會」，由宏碁資訊暨網路安全中心統籌，直接對董事長負責，委員代表包括宏碁IT產品線負責人及集團內子公司總經理，下設工作小組，負責集團資訊安全及保護相關政策制定與風險查核等，每季向董事長與總經理進行報告，每年至少一次向董事會彙報集團資安治理成效、資安相關議題及方向。




## 資通安全政策與具體管理方案

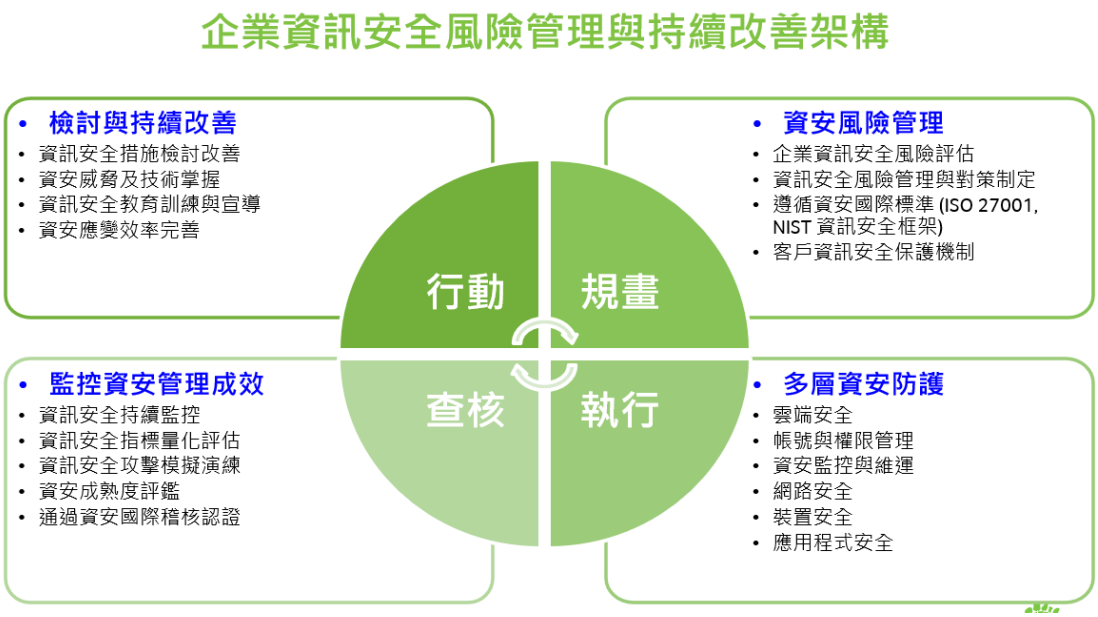
1. 企業資訊安全管理策略與架構

   企業資訊安全組織為有效落實資安管理，除了定期對管理階層和董事會進行資安管理成效和風險匯報外，並每 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 2021 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，藉由資安防禦創新技術，將資安控管機制整合入軟硬體維運及平日作業流程，利用 NIST CSF 框架來持續評估公司資安成熟度，做為強化的方向依據。

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

- 重點與執行成果
  - 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，同時納入電子商務系統 ISO27001 驗證範圍。
  - 泛歐 IT 推動重要核心系統，導入並通過 ISO27001:2013 第三方驗證。
  - 宏碁企業資訊安全組織持續發布或修訂全球 Cyber Security 細項政策，確保 Acer 全球 IT 人員、產品開發人員與子公司 IT 有執行資訊安全準則依據。
  - 持續導入與落實全球資訊安全零信任防禦與監控管理機制，強化全球資安防禦能力。
  - 完善全球弱點管理儀表板即時監控，快速概觀風險控制所需資訊，並強化修復標準，降低風險。
  - 完善全球防禦與威脅偵測資訊儀表板，即時掌握資安風險。

- 多層資安防護

| | |
|---|---|
| 裝置安全 | • 全面導入端點防護 EDR ( Endpoint Detection and Response )<br>• 端點防毒措施強化惡意軟體偵測<br>• 全面導入端點自動化 Patching 管理機制 |
| 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<br>• 與第三方合作，搜索暴露在暗網的帳號，主動變更密碼<br>• 啟動帳號可疑存取監控機制 |
| 網路安全 | • 強化網路防火牆與ACL ( Access-control list )控管<br>• 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<br>• 標準化全球網路安全設定 |
| 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<br>• 盤點過時及有風險的軟體套件，執行必要的升級 |

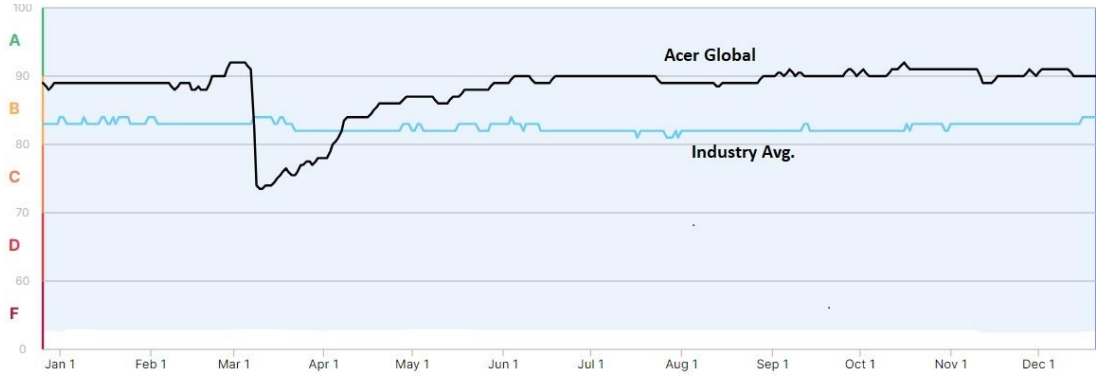
- 資安成效控管

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。

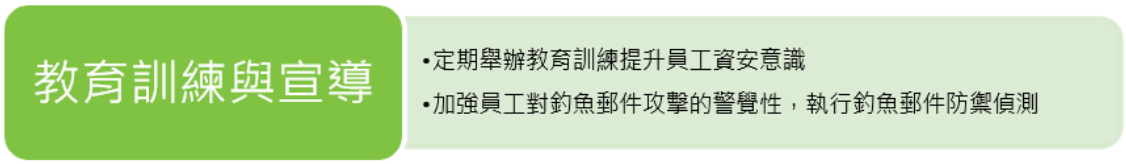
| | |
|---|---|
| 資安成熟度評鑑 | •委託外部專家執行公司網路與資訊安全評鑑 |

產業平均為藍色曲線，分數約為 82，成熟度為 B

Acer 為黑色曲線，除首季的資安事件外，保持向上態勢，2023 年 6 月後穩定居於產業平均表現之上，分數為 90, 成熟度評比維持在 A 級。

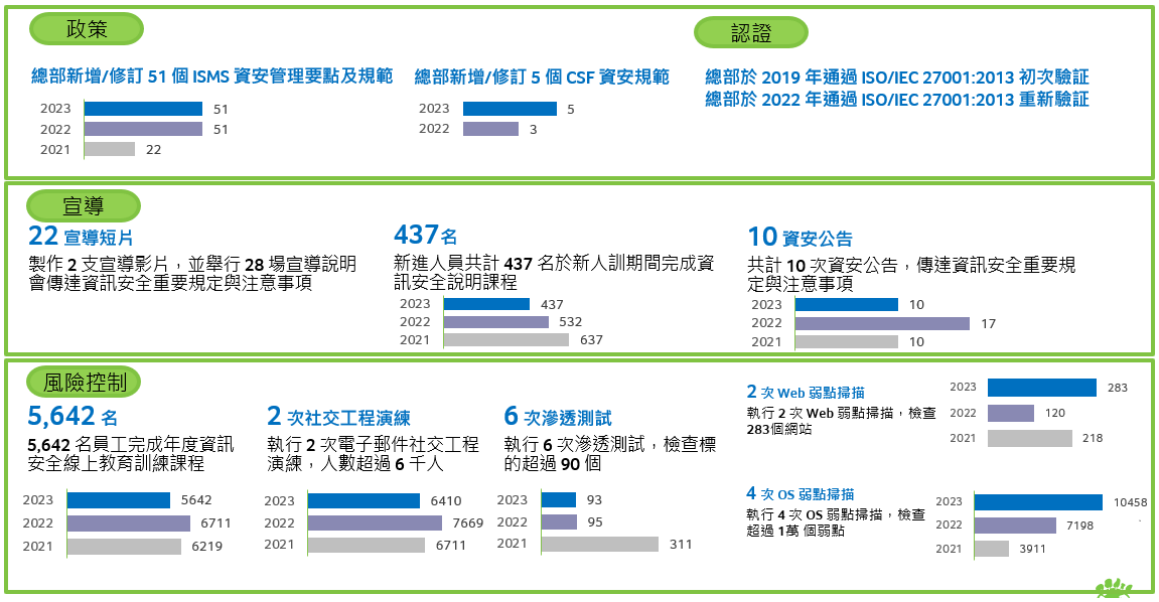


檢討與持續改善




4. 具體執行成果

民國 112 年企業資訊安全措施推動執行成果




每月執行雲端安全掃描，修復超過 4000 個弱點

**<u>民國 112 年資安管理強化重點：</u>**

- 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，並辦理 ISO27001:2022 Workshop，確保同仁認知以及控制措施依新標準升級，降低資安風險。
- 修訂資安政策與管理要點，並持續發布全球 Cyber Security 細項政策，確保組織資安作法與 ISO27001:2022 版本新規範接軌。
- 擴大 ISO 27001 管理~~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。
- 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
- 導入端點 OS 自動化 Patching 方案，強化端點安全度

**<u>第三方驗證紀錄：</u>**

- 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

- 2023/03/16 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
- 2023/09/14 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