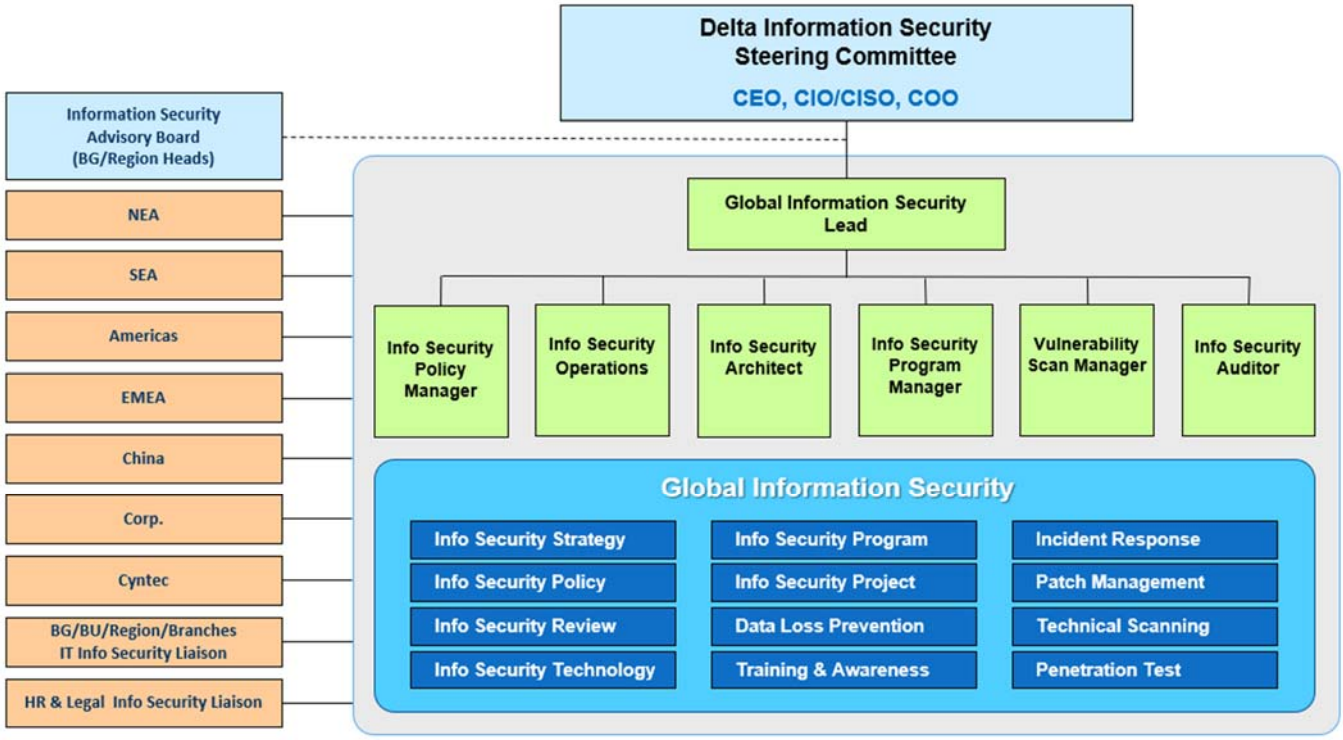
台達資通安全執行情形

台達集團已成立資通安全組織架構，並設置嚴謹的資通安全佈局及完善的資通安全管理流程，並由資訊長每年定期向董事會報告資通安全執行成果。今年度(111 年)已於 2 月 24 日由資訊長向董事會報告資安治理情形，包括二大主題 (1) 勒索軟體攻擊事件摘要報告，(2) 資通安全治理計劃說明。

(一) 企業資訊安全治理組織

台達集團已設立「資通安全委員會」，下由執行長、資訊長暨資安長、營運長監督與審查，下轄資訊處資通安全部，統籌資通安全政策管理、資通安全運作、資通安全架構、弱點管理、資通安全風險管理與遵循度查核，並於全球各地區設立資通安全負責人，以確保資通安全政策與管控落實於台達集團全球各地區事業單位。每一季由資安長向資訊安全委員會彙報資安管理成效、資安相關議題及發展方向。



(二) 資通安全政策與管理方案

台達集團於 107 年導入 ISO27001 資通安全管理系統(ISMS)並通過驗證，為維持證書之有效性，台達集團每年都接受第三方外部稽核作業，目前證書有效期為 110 年 8 月 8 日至 113 年 8 月 8 日，涵蓋 111 年度。為使制度有效運行每年定期檢視資通安全政策之妥適性；且台達集團已加入台灣資安聯盟、高科技資安聯盟等，以利取得資安相關訊息並即時獲取資安情資。

台達集團全球員工及約聘僱人員皆須遵循台達資通安全政策以及下列資安規範：

1. 資訊設備使用準則
2. 行動裝置使用原則
3. 密碼使用準則
4. 公司電子郵件使用準則

5. 網際網路使用準則
6. 資訊處理準則
7. 軟體使用與授權準則
8. 可卸除式電腦媒體裝置使用原則
9. 訪客安全準則
10. 防毒與資料外洩防護軟體部署原則
11. 遠端存取準則
12. 資安事件管理準則
13. 對外網路應用服務資安要求
14. 公司資源使用準則

(三) 投入資通安全管理之資源

1. 全球資通安全管理

九位 IT 資通安全專責人員，每月召開資安代表會議檢視公司全球資通安全議題，並於各主要單位指派共四十多位資安代表，每月召開資料外洩防護 (Data Loss Prevention - DLP) 計畫執行檢討會議。

2. 資安運營監控 (Security Operation Center，SOC)

專責團隊負責即時監控與識別資通安全事件，強化資通安全事件之應變處理。

中達電子(蕪湖)有限公司、台達電子(東莞)有限公司、達創科技(東莞)有限公司及台達電子(郴州)有限公司已於民國 109 年取得中國海關高級認證。

3. 弱點掃描與滲透測試

對台達集團之網路設備、應用系統及產品定期進行弱點掃描，對網站及系統進行滲透測試。

4. 年度資通安全教育訓練、釣魚演練

對台達集團全球員工進行資通安全教育訓練，依據各國慣用語言分為多語言版本確保教育訓練成效；於各地區執行釣魚演練、釣魚郵件辨識宣導，分析演練結果以持續提升演練有效性。

(四) 資安與隱私管理系統導入與驗證

因應各國對於個人資料保護的重視，個資隱私保護管理能力越顯得其重要性，然而若要使個人資料有妥善的保護，資訊安全便為不可或缺之防護能力。ISO27701 是一針對隱私資料安全的國際標準，為強化台達集團於全球各個國家對於資訊安全及隱私保護的管理，台達集團自 2021 年起將原本 ISO 27001 驗證範圍擴大至歐洲荷蘭及瑞士等辦公室，並同時導入隱私資訊管理制度（PIMS），以 ISO27701 為遵循原則及 PDCA 管理循環，持續提升資訊資產及個人資料的保護以降低所面臨的風險，完善台達集團對於資訊安全暨隱私保護之管理。

(五) 重大資安事件之影響及因應措施

民國 111 年 1 月，台達部份資訊系統遭受駭客網路攻擊，造成公司官方網頁與內勤工作辦公室自動化(Office Automation)與相關系統無法存取，資訊單位偵測到異常後，立即通知相關單位啟動資安應變機制，亦邀集外部資安專家協同進行事件之處置，以遏制惡意程式擴散與攻擊手法之分析調查，並且迅速盤查受影響系統進行系統復原；因此，本次事件對公司整體營運

未造成顯著影響及損失，依據法令規定本公司已向政府執法部門進行通報與發布重大訊息。

初步事件分析與調查之結果推測駭客是以社交工程之方式取得本公司員工帳號，進而透過網路入侵公司電腦發動攻擊。針對此風險，台達資安單位已規劃加強對全球台達同仁的資安教育訓練與社交工程演練，資訊團隊將加強郵件過濾機制，並持續提升網路與系統之監控及安全管控，以降低資通安全風險避免類似之駭客攻擊事件再度發生。