台達資通安全執行情形

一、 資通安全風險管理架構

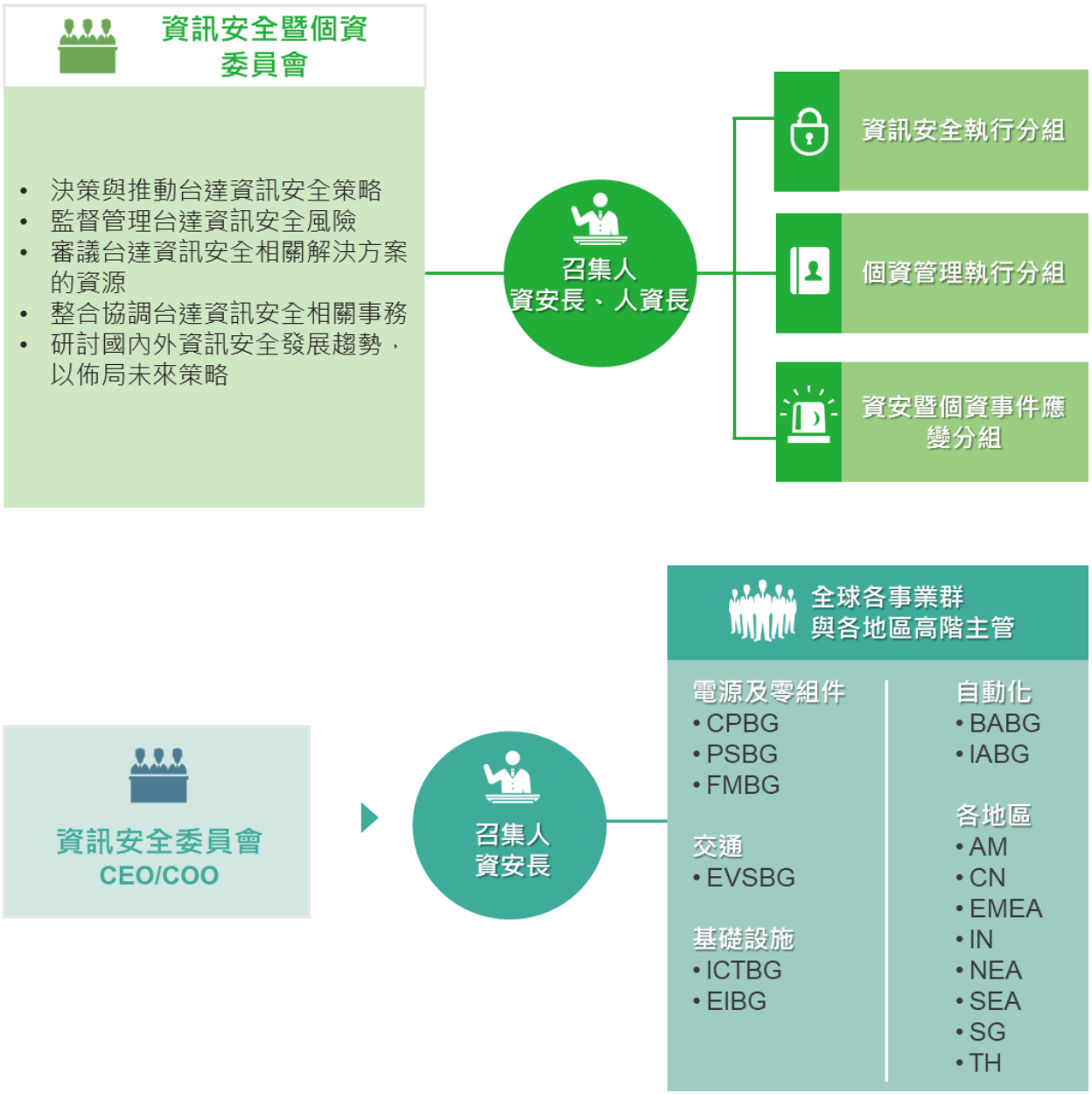
台達集團資訊安全政策及資訊安全相關重大議題之決策由董事會負責核定，審計暨風險委員會負責審查，以彰顯管理階層對於資訊安全管理制度之支持與參與。資訊安全議題同時屬審計暨風險委員會管轄之企業風險管理(ERM)的一環。透過每季向審計暨風險委員會回報資訊安全 ERM 關鍵風險指標(KRI)，持續追蹤資安機制是否有效支持企業整體風險控管策略，並強化組織韌性。民國 114 年 7 月 30 日「台達集團資訊安全暨個人資料保護政策」修正案經審計暨風險委員會審議通過後，提報董事會核准。

為有效討論和識別資訊安全相關風險，本公司成立資訊安全委員會，由執行長擔任主席並由資訊長擔任資訊安全長，全球各事業群與各地區高階主管均為委員會委員；亦成立「資訊安全部」，專責台達集團資訊安全及實體安全規劃與相關的稽核事項，並促進此委員會運行。資訊安全委員會透過每季管理審查會議，審核資安風險分析結果及本公司採取對應的防護措施與方策，確保資訊安全管理體系持續運作的適用性、適切性及有效性。資訊安全長每年定期至少一年一次向董事會彙報資安管理成效及資安策略方向，以確保資訊安全政策與管控落實於台達集團全球各地區事業單位。於民國 114 年 2 月 26 日及民國 115 年 2 月 25 日由資訊安全長向董事會報告資安治理情形。

二、 資通安全政策

台達持續精進其資訊安全制度，並強化防護能力。透過成立「資訊安全暨個資委員會」來推動整體資訊安全治理，建立一致性的資訊安全政策，並規劃台達集團之資訊安全管理制度。台達由董事會負責核定集團資訊安全暨個資保護政策，以及決策資訊安全相關重大議題。所有資訊安全管理規範不僅需要符合國內外的資訊安全法律法規，還積極擴大國際資安標準的適用範圍和認證領域，將資訊安全融入日常業務的執行中。本政策每年會配合政府法令、環境、業務與技術之變動評估檢討，其修正須經董事會核定後公告實施。每年亦會針對集團員工，實施資訊安全政策及認知宣導，以加強同仁資訊安全意識。

資訊安全暨個資委員會組織圖



三、 具體管理方案

為達資安政策與目標，建立全面性的資安防護，推行的管理事項及具體管理方案如下：

(一) 組織控制

- 台達訂立「台達集團資訊安全暨個人資料保護政策」，做為資訊安全暨個資管理組織權責分工、人員教育訓練、電腦硬軟體、網路及實體環境管理之準則。
- 台達主要資訊系統於民國107年12月3日通過ISO/IEC 27001驗證，為持續確保資訊安全實施與維護證書有效性，每年實施包含資產盤點、風險評鑑與處置、關鍵系統營運持續演練、資訊安全事件演練及內部稽核等控制措施。經外部驗證單位於民國113年7月12日以ISO/IEC 27001:2022 國際標準執行驗證通過，並於民國114年9月5日完成監督驗證，現行證書有效期限至民國116年8月8日。我們將持續推動與落實資訊安全制度至台達集團全球各地區、各事業單位，以降低未知的資安風險，建立一個安全可信賴的資訊環境，從而保障集團和客戶的權益。
- 為了確保資訊安全管理文件能夠與組織的實際運作相符合並因應資訊技術的不斷演變，確保它們能夠有效地反映台達的最新需求和資訊安全標準，台達在民國114年修改共計9份程序文件，並新增1份表單。完成

並通過客戶資安問卷或內部、外部審查共計86件。此舉措反映台達在優化、加強既有流程、配合客戶及外部稽核要求等需求上的積極與努力，透過致力於持續提升其資訊安全管理水準，確保其資訊系統和資料得到妥善保護。

- 透過國際資安大廠提供之專業服務進行整體資安體檢，以公正第三方驗證之客觀結果，作為進階資安強化的依據。
- 台達的資安服務廠商提供資安情資，以強化現有威脅偵測解決方案，並加入台灣電腦網路危機處理暨協調中心(TWCERT/CC)，不定期收到資安情資，分析整合現有情資來提升防禦效率，以進行適當防範，降低公司可能暴露之風險。

(二) 人員控制

在當今數位化和資訊化的環境中，資訊安全教育訓練被視為至關重要的一環。透過充分的資訊安全意識培訓，員工能夠更好地理解資訊安全的重要性，並學習如何預防和應對各種資安威脅。這包括學習如何避免常見的人為錯誤，並確保遵守相關的法規和標準。擁有這些資訊安全意識的同仁可以大大減少組織面臨的安全風險，提高數據和系統的保護水平，從而確保組織的業務運作安全可靠。

- 台達除對新進員工進行資安教育訓練，專業技術及管理單位人員亦須完成年度資訊安全教育訓練並通過測驗，民國114年共提供9個語言版本，共計 41,689人次完成年度資安線上與實體教育訓練，完成率 99%。資訊安全部亦會不定期發行資安電子報或資安相關課程，提醒員工最新的資訊安全風險、員工應注意事項等，民國114年共計發送7封電子報 ，辦理課程共計12堂。資訊安全部也設有資安專屬信箱，以利同仁發現資安問題時可即時反映。
- 為提升同仁資訊安全意識，每年定期對全球員工舉辦社交工程釣魚郵件演練、釣魚郵件辨識宣導，並分析演練結果以持續提升演練之有效性。演練情境配合發送區域提供多國語言版本，並依趨勢選用常見釣魚手法，例如：密碼到期變更要求、通訊軟體群組邀請等憑證釣魚模擬郵件，AI工具使用邀請，以及夾帶附件的誘導互動類型釣魚模擬郵件，以訓練員工對於識別和報告不同釣魚郵件的能力，及識別需加強資安意識提升之員工。民國114年共執行24次釣魚郵件演練，共寄出 93,659 封郵件，社交工程與釣魚郵件認知宣導課程完成人次共計6,157，共計通報釣魚郵件數量為45,555封，其中11,282封為正確識別出釣魚演練信件。

(三) 技術控制

- 維運防毒與端點防護系統，並搭配多層次資安監控機制，防止電腦病毒及惡意程式入侵風險。
- 佈署SIEM(Security Information and Event Management)系統及端點偵測與回應(Endpoint Detection and Response)工具，以提升資安威脅偵測與回應的效率。事件平均偵測時間小於24小時. 並具備每月防禦約200萬次攻擊嘗試的能力。
- 建構次世代網路防火牆來達成網路防護與區隔，以強化關鍵基礎服務之安全管控措施。
- 佈署郵件安全閘道器Secure Email Gateway (SEG)，以阻擋駭客發送內含惡意程式或連結的釣魚郵件。
- 實時監控對外資料傳輸資料，以識別和管理潛在的資料外洩風險。
- 針對佈署於公司的應用系統，進行弱點掃描與管理，並因應數位化轉型與雲端安全性，推動更多的自動化整合方案以加強資安韌性。

四、 投入資通安全管理之資源

資訊安全已為公司營運重要議題，對應資安管理事項及投入之資源方案如下：

- 專責人力：設有專職之資訊安全主管 1 人及「資訊安全部」15 人，負責本公司資訊安全規劃、資安系統運作、技術導入與相關的稽核事項，以維護及持續強化資訊安全。
- 台達成立了「資訊安全委員會」，由執行長擔任主席，資訊安全長擔任召集人，營運長及全球各事業群與各地區高階主管均為委員會委員；每季定期召開會議，探討各地區面臨的資訊安全問題及業務需求並決定所需資源及執行方案。
- 台達於民國 112 年成立了「資訊安全推動委員會」，由各事業群指派主管擔任資訊安全推動種子，於定期的雙月會中，除了討論資訊安全相關議題外，亦透過此會議宣導總部正在推廣之資訊安全活動，藉此提升同仁資訊安全意識。

五、 重大資安事件之影響及因應措施

對資訊安全事件的通報與處理，台達已明確訂立資安通報及處理流程，資安事件由資安維運管理小組進行收錄並訂定事件等級。相關單位需於目標處理時間內排除及解決資訊安全事件，並在事件處理完畢後進行根因分析與採取矯正措施，以預防事件重複發生。民國 114 年本公司未發生造成公司及顧客損失之資訊安全事件。

民國 115 年 2 月，本公司海外子公司部分系統受到網路攻擊，並有部分業務相關資料及員工個人資料外洩之風險。資訊單位於偵測到異常情形後，立即通報內部相關單位啟動資安事件應變機制，並同步偕同外部資安專家進行事件處置作業，包括執行系統隔離、啟動防禦措施、主動阻斷惡意連線。受影響系統經全面檢查並確認防護機制正常後，即恢復系統運作。本次事件對公司整體營運未造成顯著影響及損失，亦依據法令規定向主管機關通報並發布重大訊息。台達將持續完善網路與資訊基礎架構、提升異常行為監控及存取控管，強化整體防護能力，以應對日益嚴峻之資安威脅與風險，確保資訊安全。