盛群半導體股份有限公司

資通安全政策

公司的資安相關資產分為五大類：設備（Devices）、應用程式（Application）、網路（Network），資料（Data）與人員（User），針對這五大類來規劃資通安全策略。

一、 設備（Devices）：控管公司端點的硬體，許可的裝置才能接入網路，以降低不明裝置所引發的風險；作業系統即時更新，以阻擋漏洞攻擊；作業系統安裝防毒軟體，阻絕病毒與惡意程式；監控端點安裝的軟體，以便做軟體盤點。

二、 應用程式（Application）：採用多因子驗證，以確保身分識別（Identify）；引進Web Application Firewall（網站應用程式防火牆），以有效阻擋針對應用程式的攻擊；建立叢集架構（Cluster）以確保應用程式的服務。

三、 網路（Network）：遠端連線，採用多因子認證以確保身分識別（Identify）；引進新世代防火牆，依應用程式來進行管理；入侵偵測系統以及早發現攻擊；採用進階威脅偵測、防護技術，以防止未知威脅。

四、 資料（Data）：機密資料，進行加密，以防止資料外洩；資料存放在專門的儲存設備，以免資料因硬體故障流失；專業備份軟體與設備，每天進行資料備份，並同時備份一份至遠端。

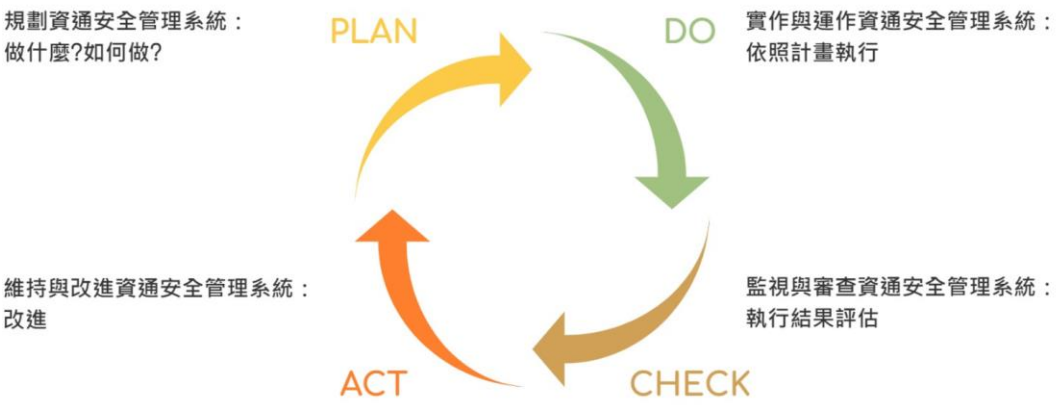
五、人員（User）：分為一般員工與資訊人員

(一)一般員工：新人教育訓練，以提高資通安全意識，提升整體的防禦能力；不定期進行社交工程演練，以加強資通安全意識，並找出資安意識較弱的同仁，以進一步的教育訓練。

(二)資訊人員：參加資通安全教育訓練、資通安全大會以提升資通安全能力；引進特權帳號管理系統，以降低風險。

資通安全策略的執行：

採用規劃—執行—檢查—行動（Plan-Do-Check-Act , PDCA）模型，並整合風險管理週期來進行。



風險管理週期

i. 識別（Identify）：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。
ii. 保護（Protect）：建立和實施適當的安全措施以確保重要服務的運行。
iii. 偵測（Detect）：制定並實施適當的作為以識別網路安全事件的發生。
iv. 回應（Respond）：對偵測到的網路安全事件，規劃並實施適當的行動。
v. 復原（Recover）：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。

如何決定資安政策執行優先順序：

採用 CSF 中有明確的提出 7 個步驟，協助組織進行資安風險評鑑，並依照框架來判斷資安成熟度，先篩選出符合組織所需的資安控制措施，再將組織間的資安風險進行排序，優先處理較為嚴重的資安漏洞，並建置完整的管理週期，一步一步的提升整體的資安成熟度。

Step 1：確定優先級和範圍。
Step 2：確認組織目標與方向。
Step 3：描述當前資安狀況。
Step 4：進行風險評估。
Step 5：描述目標資安狀況。
Step 6：確定、分析差距並確定其優先級。
Step 7：實施行動計劃。