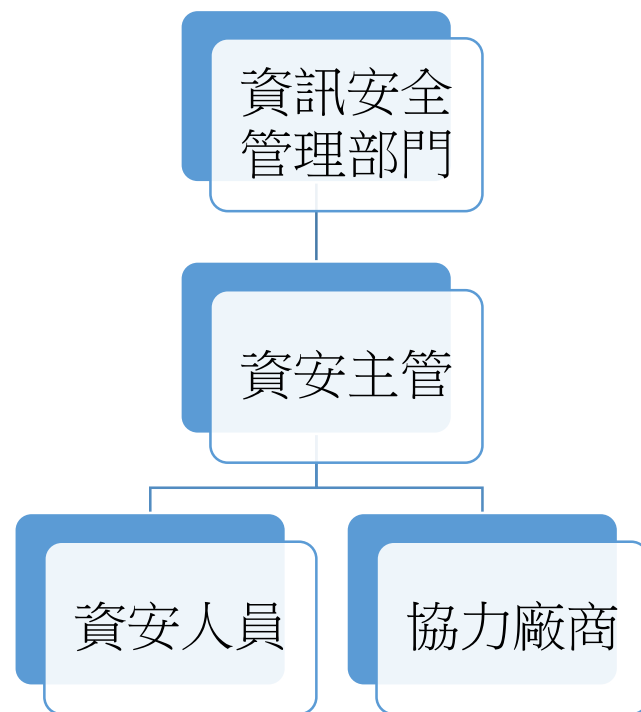


# 資安管理組織架構



# 資安單位的功能

## 管理制度與資安合規遵循

- 建立符合稽核和資安合規要求之資訊安全策略、管理制度與資訊安全發展方針。
- 監控與確認資訊安全控管之有效性，確保資訊安全制度永續運作。
- 持續追蹤海內外資安合規要求，並更新管理制度。

## 專案管理與委外管理

- 配合業務單位之需求，建置資訊安全最佳實務。
- 配合電腦鑑識與法律遵循之活動。
- 跨部門資訊安全事務之協調，以及溝通與宣導資訊安全管理要求。

## 資安風險管理

- 發掘潛在資安風險及需求。
- 定義與管理風險管理程序。
- 提供業務單位相關風險諮詢服務，與提供風險管理解決方案。

## 資安解決方案評估

- 協助資訊安全產品之選擇。
- 提供資訊服務安全和相關解決方案之專業技術研究與諮詢服務。

## 資安檢視與監督

- 檢視、覆核資訊安全發展成效。
- 配合企業策略與法規要求，評估相應之資訊風險與可能之控管。

## 威脅與弱點管理

- 蒐集與管理外部網絡攻擊威脅與內部弱點之情報。
- 建立IT基礎架構和應用程序的弱點管理服程序。

## 資安監控

- 基礎架構和應用系統之稽核軌跡留存之定義、調整與等規劃管理。
- 監控及分析日誌，調查與處置疑似異常之行為。

## 事件應變管理

- 資訊安全事件監控與反饋，包含蒐集資訊安全事件相關資訊並反饋於監視作業中、彙整疑似資訊安全風險項目、主動通報資訊安全事件。
- 攻防演練規劃、執行結果追蹤與改善檢討。

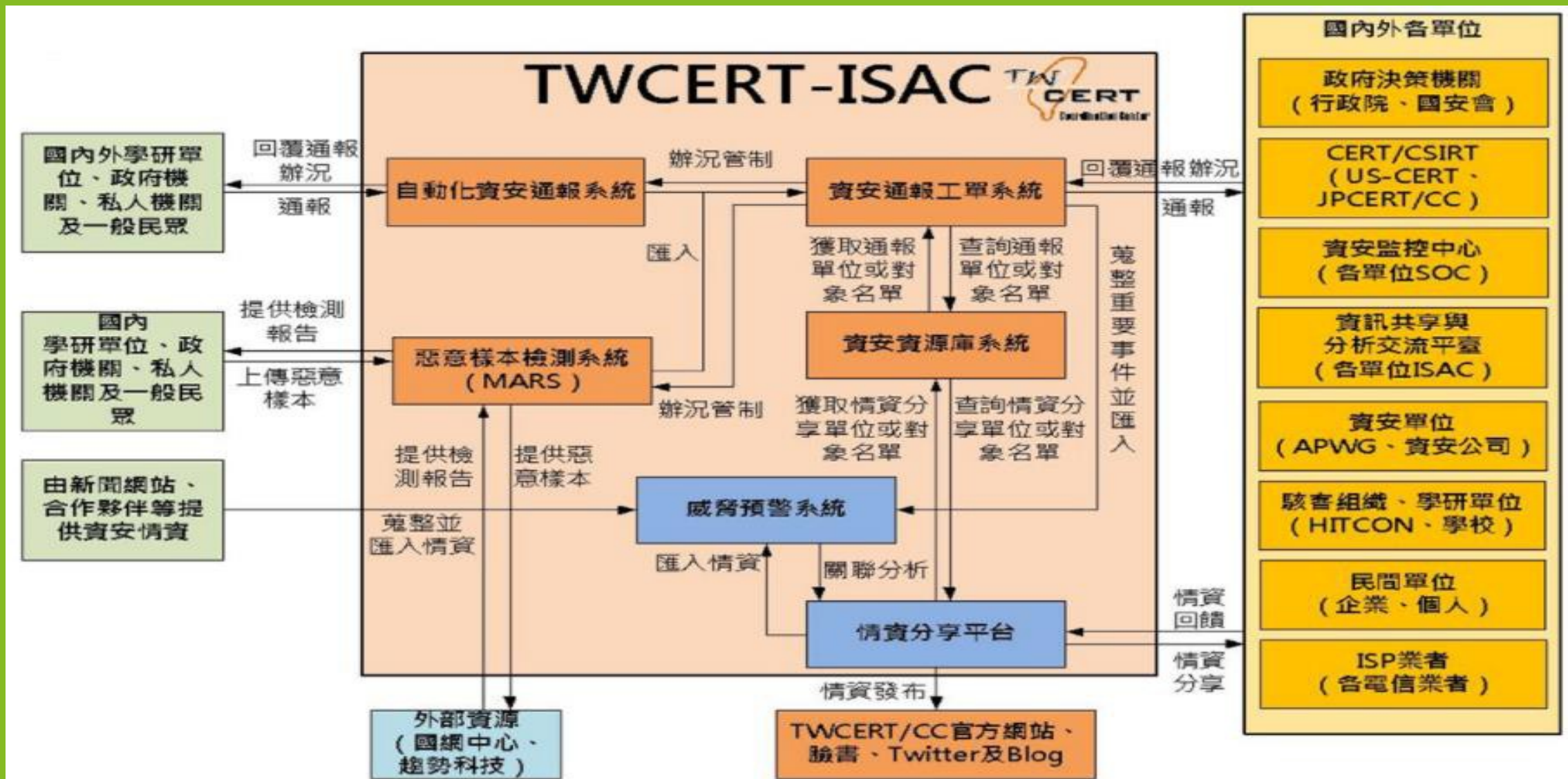
## 數位鑑識

- 蒐集異常活動之紀錄，支援鑑識需要
- 鑑識資料之蒐集分析及保存
- 產製定期報告

## 資安稽核

- 辦理資訊安全內、外部稽核活動，與追蹤相關改善措施。

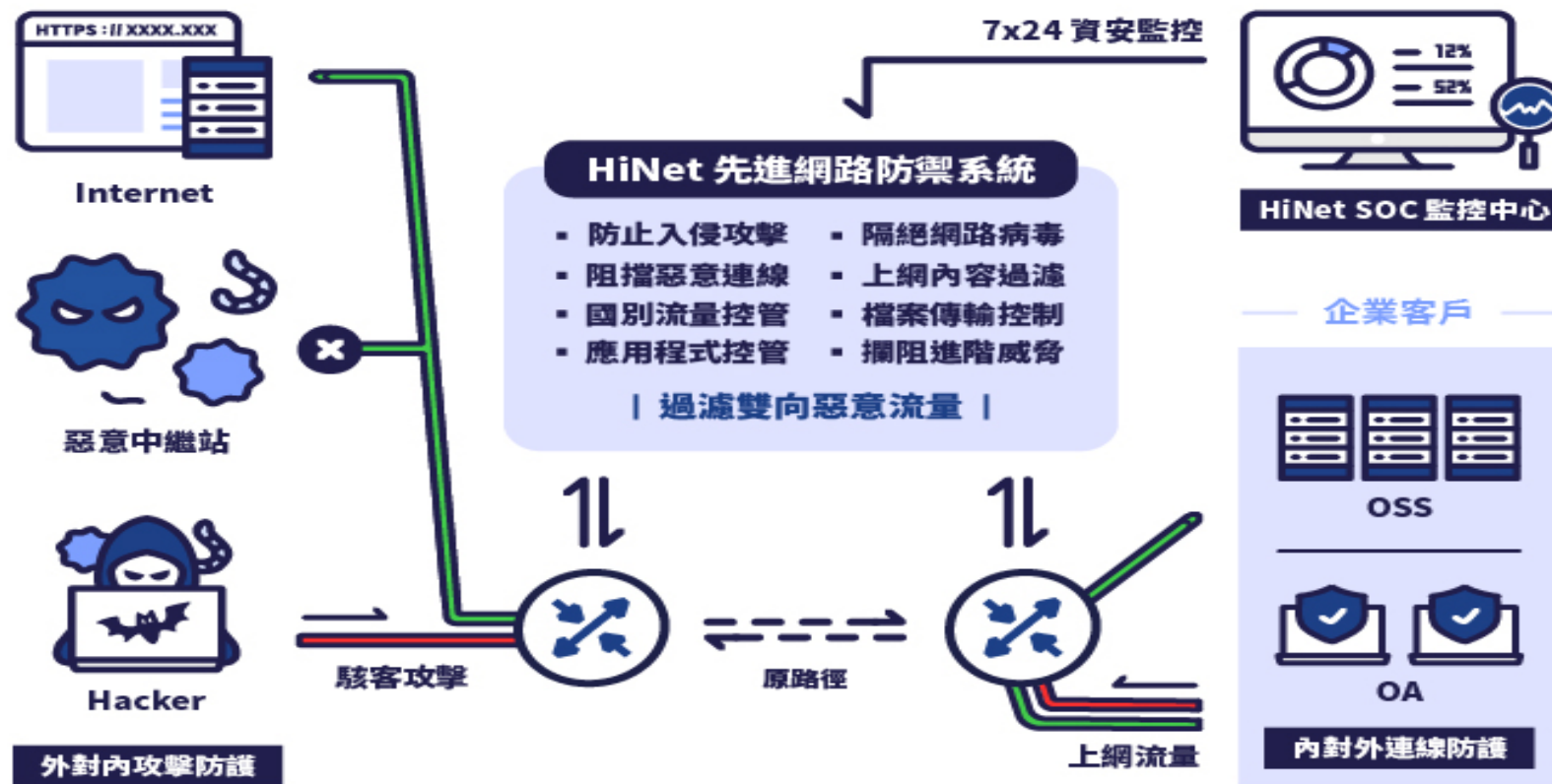
# 加入ISAC、TWCERT資安情資分享平台共享資源



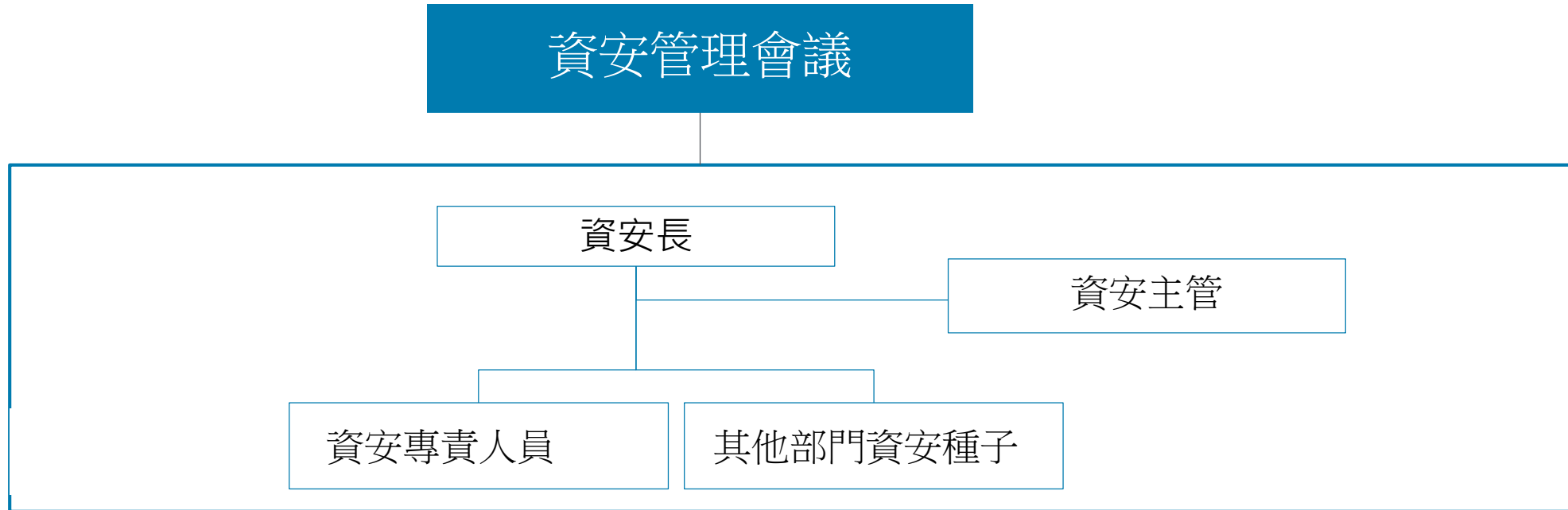
資料來源：TWCERT/CC

# 加入中華電信ANDS 先進網路防禦系統

## HiNet 先進網路防禦系統架構示意圖



# 定期召開資安會議



會議內容：

- 討論與議定全公司資訊安全之重大事項。
- 督導各項管控措施之實施，評估可能面臨威脅與潛在風險。
- 覆核資訊安全風險評鑑報告，決定可接受之資訊安全風險水準。
- 考量公司營運需求、資訊安全需求、技術變遷等因素，審議及公布資訊安全政策、資訊安全目標及資訊安全相關規範，以確保資安制度持續有效地運作。
- 督導重大資訊安全事件之應變處理與改善措施。
- 檢討並改進現行資訊安全管理制度，以提高其運作效率及有效性。

# 資通安全政策

## ◆政策說明：

- 為有效推行資訊安全管理制度，以確保資料、系統、設備及網路安全、設備及網路安全，本公司訂定有資訊應用相關之電腦軟硬體管理規定、系統主機管理規定、及資通安全相關評估辦法，做為資訊安全管理工作之執行、評估及稽核指引，以確保本公司各資訊系統可持續性運作、所屬資訊之完整性、有效性、可用性、及安全性，並落實遵守資通安全相關法律及規定。

# 具體管理方案及投入資通安全管理之資源

- 各項資通安全政策及具體管理方案說明如下：
  - 1.資通安全管理政策
    - 為確保本公司資訊安全，每年依資通安全稽核查檢表，針對資訊安全政策、組織安全、資產分類與控制、人員安全、實體與環境安全、通訊與作業管理、存取控制、系統開發與維護、營運持續管理、相關法令符合性等事項進行評估，並由稽核單位抽樣複查。
  - 2.資通安全管理措施
    - (1)機房及電力：管制人員進出、進行環境監控、進行環境監控、並定期檢測不斷電系統 檢測不斷電系統。
    - (2)主機管理：導入虛擬化容錯移轉之備援架構，以避免故障影響，同時定期完整備份資料及執行異地保存等，訂定明確的管理規範，並依規範定期實施復原演練
    - (3)網路管理：內部設置有防護機制，進行 VPN 管制及使用通知 VPN 管制及使用通知，對各主要設備皆規畫有對應之備援設備，以減低故障影響，同時租用經認證之網路攻擊防護、垃圾信件過濾及信件病毒過濾防護、(中華電信資安艦隊)服務，進行雙重防護。

# 具體管理方案及投入資通安全管理之資源

- (4)電腦管制：導入電腦資產管理系統，即時管制全公司電腦，掌握電腦的異動、電腦軟體的合法使用，強制防護軟體的啟用，及報廢的處置。
- (5)帳戶管制：各系統使用權限皆需經申請及簽審核，人員調離職的權限檢視，並每年定期複查驗人員權限。
- (6)系統發展：針對系統之作業權限、存取管理、功能變更、問題處理等，訂定明確的作業程序與規範。
- (7)教育推廣：平時交機使用旋即進行資安觀念宣導，定期執行新人訓練資安訓練宣導，同時不定期公告高風險資訊，提醒員工加強資安觀念。
- (8)組織管理：專職資訊管理部門及人員，並定期向經營最高主管報告執行運作狀況。