亞洲航空股份有限公司
資通安全風險管理架構及管理作為

資安風險管理架構：

一、本公司設置資通安全委員會，以資通安全政策為依歸，定期制定/檢討各項資通安全管理辦法與指標。

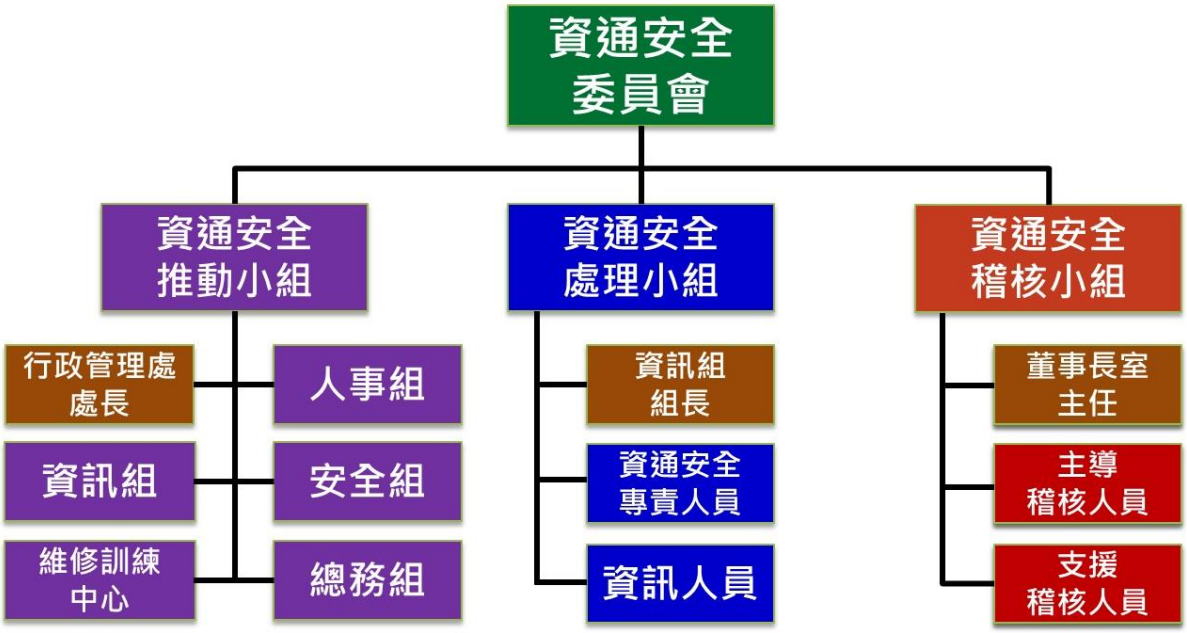
二、資通安全委員會組織

(一)資通安全委員會：委員會由行政管理副總擔任資通安全長，依資通安全任務分設各小組，相關業管部門副總/廠長/處長/主任為各單位成員；主要為建構、推展、監督與管理資通安全工作。委員會成員: 行政管理副總、軍機事業部副總、直昇機事業部副總、董事長室主任、各軍機事業部門廠長/處長、行政管理處/品保處/財務處/採購處處長、資訊組長；行政管理處處長為執行祕書。

(二)資通安全推動小組：由行政管理處處長擔任組長，納編資訊組、人事組、安全組、總務組、維修訓練中心；主要為執行資通安全相關之推動性工作（資通安全維護計畫擬訂、資通安全事件通報及應變、資通安全教育訓練）。

(三)資通安全處理小組：由資訊組組長擔任組長，納編資通安全專責人員及資訊人員；主要為執行資通安全相關之技術性工作（安全性檢測、資通安全健診、資通安全威脅偵測管理機制、資通安全防護）。

(四)資通安全稽核小組：由董事長室主任擔任組長，納編完成ISO27001主導稽核員訓練人員以及支援稽核人員(品保)為小組成員；主要為執行資通安全管理系統之稽核作業。



資安風險管理運作：

一、強化資安管理，並配合政府推動「國防產業發展條例」，導入ISO27001(資訊安全管理系統)且取得認證。

二、派員參與「ISO27001主導稽核員認證」專業課程並取得證照。

三、依「ISO27001(資訊安全管理系統)」落實資通安全管理各項作為，包括：

(一)編寫「ISMS資通安全管理手冊」為資通安全管理之準則，確實各項資通安全之執行。

(二)制定各項管理辦法：個人及公用電腦設備管理規範、資訊資產管理辦法、電子郵件信箱管理規範、資訊業務持續運作管理辦法、實體安全管理辦法、緊急應變計畫、資訊安全查核辦法、系統復原計畫、存取控制管理辦法、系統開發與維護管理辦法、資訊委外作業安全管理辦法、電腦機房維運作業管理辦法、資通安全風險管理辦法等。

(三)風險的控制與實施(資訊技術之引進與施行)：引進/設置防火牆系統，可有效阻隔來自廣域網路的各式攻擊，實施微軟AD帳密複雜性規範，設置企業級防毒軟體、郵件過濾/偵測系統、儲存系統備援機制、資訊安全通報機制。

(四)風險之檢討與改善(資安執行成果檢討)，加強宣導強化同仁資安觀念與執行，不定期實施弱點掃瞄、針對缺失加以研究改善。

資安風險管理作為：

一、資訊系統建立備援機制。

二、每日執行主機及資料庫備份，每日機房查核並記錄。

三、設置防火牆建立內/外網之區隔。

四、每年執行二次資通安全內部稽查。

五、每年召開一次管理審查會議。

六、每年至少一次營運持續演練計畫。

七、每年至少一次系統弱點掃描及滲透測試。

八、每年安排同仁資安訓練課程。

九、不定期對同仁進行社交工程測試。

十、不定期資安宣導。

資訊安全具體管理方案：

一、帳號/權限之管理與審核

(一)帳號/權限之申請或變更均需經過行政簽核系統核定，並不定期複核。

(二)密碼配合微軟AD網域實施複雜性原則設定，90天需變更一次密碼，強制執行密碼歷程紀錄以及最小密碼長度。

二、存取管制

(一)限制資料/檔案對網際網路的上/下傳送(需經申請/審核/查驗)。

(二)限制可移動式裝置(如USB、光碟機、燒錄機)之使用(需經申請/審核/查驗)。

(三)應用程式以權限控制資料的輸出/入。

三、多層次防禦

(一)設置硬體式防火牆，封包過濾功能可有效阻絕外部的攻擊與滲透並記錄攻擊的來源與行為可做為入侵檢測的分析數據。

(二)郵件記錄主機，內含郵件過濾功能及掃毒功能。

(三)在公司內部網路每部電腦皆安裝有端點防護軟體(具有防毒、防駭功能)。

(四)每年至少一次主機弱點掃瞄檢測。

四、系統可靠度

(一)主機採高可用性虛擬化架構，可有效降低停機時間、系統可自動備援，主動的風險迴避。

(二)每日資料備份並每年進行「資訊業務營運持續演練」，確保系統穩定運作。