出國報告（出國類別：實習）

新加坡 IATA 航空保安訓練視訊課程結訓報告

服務機關及姓名職稱：交通部民用航空局 邱美珍 技正
交通部民用航空局 郭姿佑 專員
中華航空公司 吳桂菱
長榮航空公司 蔣侃倫 課員
華信航空公司 林維庭 稽查員
星宇航空公司 詹媛 專員
桃園機場公司 駱英吉 專員
凌天航空公司 尹絜 主任

派赴國家：線上課程

出國期間：2022 年 5 月 23 日至 5 月 26 日

報告日期：2022 年 6 月 22 日

摘要

財團法人中華民國台灣飛行安全基金會（以下簡稱飛安基金會）配合民航政策，藉協調、支援與輔助功能，促進提升整體飛安系統運作順暢。按國際民航組織、政府政策與航空業界之需求，並就專業師資與課目教學需求而考量，每年選擇相關課程，派遣適員參加訓練，以擴大航空產業視野與接軌國際。

為培育航空保安人才，降低航空保安異常事件，強化危機解決能力，由飛安基金會薦選及贊助航空界相關從業人員參與本次「新加坡 IATA 航空保安訓練視訊課程」。參訓者為交通部民用航空局邱美珍、交通部民用航空局郭姿佑、中華航空公司吳桂菱、長榮航空公司蔣侃倫、華信航空公司林維庭、星宇航空公司詹媛、桃園機場公司駱英吉、凌天航空公司尹絜，共八員。因新冠肺炎影響，課程訓練以視訊實施，自 2022 年 5 月 23 日至 5 月 26 日，為期四天課程，學員來自亞洲各地齊聚線上。

本次課程由 IATA 資深講師，透過互動式的線上視訊軟體，帶領學員認識保安管理系統（SeMS）的全貌。瞭解 IATA SeMS 的基本要項及核心要素，並從管理角度切入，認識保安文化的建立、緊急應變的計畫、危害級脆弱點的評估、風險的管理及人為因素的影響；另外，從品質管理的方向探討品質管理的實施、SeMS 的品質保證及符合 IOSA 規範的實施方法。

目次

壹、 目的

航空保安一直是飛航安全的重要課題之一，對於層出不窮的保安事件，被動的應對保安威脅及挑戰，將導致應接不暇，防不勝防；而透過保安管理系統（SeMS）的運用，將提供一個操作原則和指導框架，以系統化、架構化及標準化的觀念，配合以資料為基礎的風險管理方式，主動管理風險及危害，並識別可能造成負面影響的漏洞，而得以提高整體安全。

貳、 課程規劃

一、授課講師

本次課程講師為 Stephen Ackroyd，來自英國。現為 IATA 外部講師和 Avsec Resilience Ltd 的董事及首席顧問。曾任教於 Buckinghamshire New University 指導航空保安碩士，並在 British Midland International 擔任航空保安主管，管理歐洲、中東、非洲等航線。

二、課程表

自 5 月 23 日至 26 日，為期四天。上課時間為 1200-1400 及 1500-1700（UTC+8），每天 4 小時，共 16 小時。

時數	5/23 Mon. Day1	5/24 Tue. Day2	5/25 Wed. Day3	5/26 Thu. Day4
1hr	Introduction & Course Overview 導論和課程概述	Security Threats and Vulnerabilities Assessment 保安威脅和脆弱點評估	Change and Project Management 改變和專案管理	Emergency, Incident Management and Contingency Planning 緊急情況、事件管理及應變計畫
1hr	IATA's SeMS Initiative and Core Elements of SEMS IATA SeMS 基本和核心要素	Security Threats and Vulnerabilities Assessment 保安威脅和脆弱點評估	Security Risk Management 保安風險管理	Security Quality Control 保安品質管制
1hr	Scoping SeMS and Performance-based Indicators 界定 SeMS 及性能指標	Building Security Organization 保安組織之建立	Occurrences Reporting and Human Factor 事件報告和人為因素	IOSA
1hr	Corporate Commitment 企業文化	Resource Management 人力資源之遴選運用	Case Study 案例研究	SeMS Implementation & course close SeMS 實施 & 結訓
自主學習	Risk Management 風險管理	Project Management 專案管理	Quality/IOSA 品質/IOSA	

三、教學方式

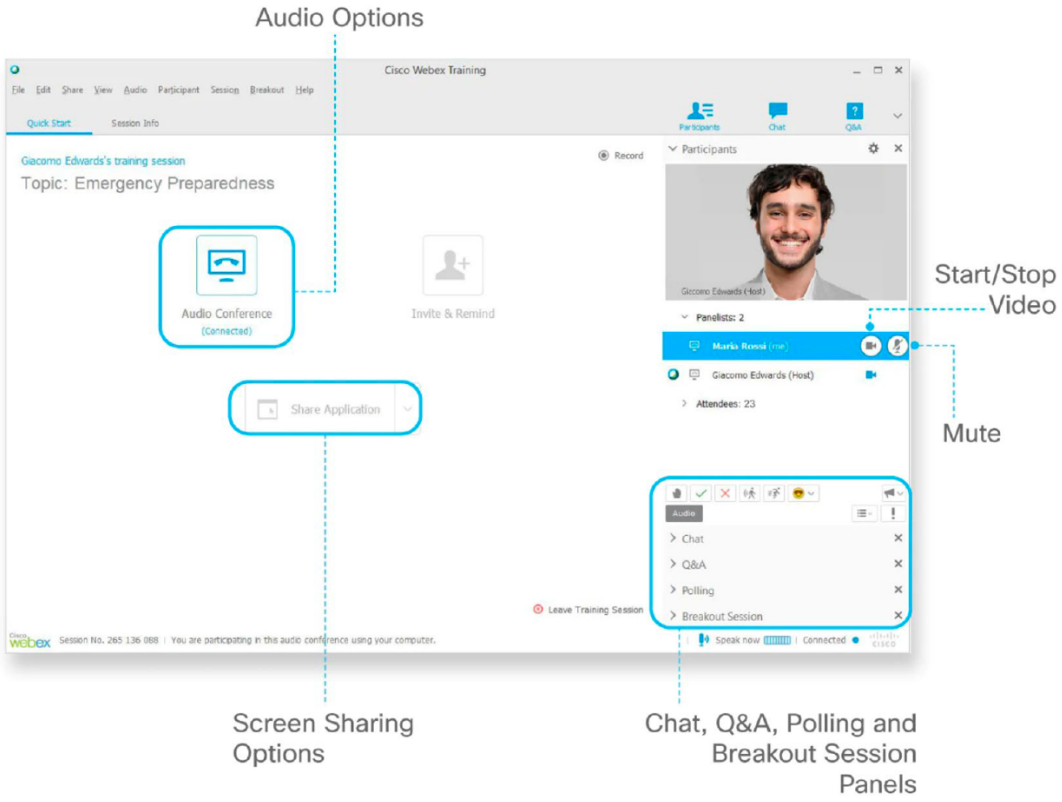
因新冠肺炎疫情影響，本次課程以視訊教學（Virtual Classroom）進行。

1. 課前

   課程協調員（Training Coordinator）在課程開始前三週開始以 Email 聯絡每位學員，確認出席及學員個人資訊。課程前一週，課程協調員會提供課程資訊，如講師資訊、課程連結、講義電子檔案、手冊電子檔案、評分方式、視訊軟體使用說明及線上考試系統教學等資訊。

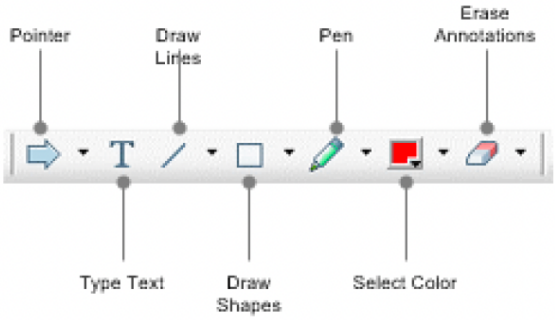
2. 課間

   使用 Cisco Webex Training 軟體，可使用電腦或行動裝置上課。但仍建議以電腦版登入，軟體功能較為齊全，以下以電腦版軟體做介紹：



課程簡報會投影在上圖左側視窗，而為了連線順暢，講師及學員全程均不開視訊鏡頭。除了以語音溝通外，可透過上圖右下角的互動欄位，使用圖示進行互動，或文字聊天。講師會在聊天視窗（Chat）適時分享縮寫全名、參考連結和參考資料等。

若使用上圖的圖示互動欄位，可舉手問問題，表示同意或不同意，或請講師語速放慢等，也可透過 emoji 咖啡圖示表示離席。



而在課程簡報投影處，講師時常會要求學員以上圖的註釋工具在公開閱覽的簡報畫面中表達個人意見。

當學員滑鼠移開 Webex 視窗，講師會收到訊息通知，系統也會紀錄時間，將會影響出席率的計算。

3. 課後

除了每天 4 小時的正式課堂外，講師會在午休的半小時回到線上，給予學員答疑解惑的時間。若學員沒有問題，講師會做課外的案例分享，此段時間不計出席，也不在測驗範圍內。

另外，每天的教材包含與當天課程相關的參考資料，作為課後自主學習用，參考資料不在測驗範圍內。

四、評分標準及完訓資格

評分項目	佔比	內容	完訓資格
測驗	50%	考試時間為 1 小時的線上單選題測驗，開書考且不監考。	總分 80 分以上為及格，90 分以上則為成績優良（Pass with distinction）。
個人習作及小組討論	30%	前三天的午休分別公布三個主題，第三天課程實施小組討論。	
出席率	20%	根據 Webex 系統紀錄。	

參、 課程內容

一、導論與課程概述 Introduction & Course Overview

本次課程目標希望學員在完訓後，可以理解 SeMS 的組成架構，並根據安全職責規劃組織結構，將 SeMS 與其他作業領域相連結；和將 SeMS 應用於程序和操作中，制定方法來建立安全意識和安全文化；且可以研擬監控 SeMS 有效性的流程。

介紹評分標準及完訓資格。

二、IATA SeMS 基本和核心要素 IATA's SeMS Initiative and Core Elements of SeMS

反思以往傳統的保安觀念，終將造成保安方面的疏漏，如利益相關者之間往往缺乏溝通和合作，尤其是政府機關與航空公司之間；保安資訊保密，且相關的風險管理僅由政府機關執行；保安沒有被視為航空的組成部分，而是由外部進行管理；不僅是被動的，且僅專注於滿足最低要求。

為改善以往的處境，透過 SeMS 系統化、標準化、組織化的保安管理模式，整合組織文化，提供目標依循，將保安管理融入日常作業中；提供必要的組織架構，責任與義務的歸屬、政策和程序，用以確保有效的監督。SeMS 作為一種安全保障系統，用以協助使保安流程更有效執行、更主動發覺且更廣泛連結。

SeMS 基本訴求就是要符合規範，並秉持著主動積極的精神進行。該系統是圍繞著風險及危害管理所建立，並為求最佳實踐而建立標準，期許可以有效率的解決保安問題。而所有的流程及程序都應紀錄備查。SeMS 是 IATA 成員及 IOSA 認證的必要符合項目，體現一個組織在保安層面上的能力。其必須融入組織的作業流程中，且需有組織文化的支持與推行，才能發揮成效。

SeMS 的文件指引可參考 IATA 的 SeMS 手冊，自 2017 年發布 SeMS 手冊第一版，至今最新版本為 2021 年的第五版。而 ICAO 則是在 Doc 8973 文件中的 9.3 節中，另諸如 UK CAA 及 ECAC 等都有針對 SeMS 的文件指引。

三、探討航空保安管理系統及績效指標 Scoping SeMS and Performance-based Indicators

1. 學習目標及主題

   (1) 學習目標：能明確說明航空保安管理系統的面向(Dimensions)及要素(Elements)

   (2) 包含三大主題：航空(Aviation)係由系統組成的系統、管理系統的三大面向，及管理系統的要素

2. 主題一：由系統組成的系統

   (1) 系統(Systems)的定義：依據牛津英文字典，係指一組事物在一起作用，形成一套機制或互連網絡；航空公司就是這樣運作的。

   (2) 企業的組織管理系統(Organizational Management System)，可能包含了許多子系統，例如飛航安全管理系統、航空保安管理系統、品質管制系統、企業風險管理系統等，內部各作業單位亦有許多系統，例如航務管理系統、客艙管理系統、簽派管理系統、機務管理系統等。

3. 主題二：管理系統的三大面向

   (1) 大多數的系統係由兩個面向構成，包含組織面(Organizational)及作業面(Functional)：

Organizational 組織面	•Leadership, team & management staff •Operational control and supervision •Resource allocation – people, finance	•領導階層、團隊及主管階層 •營運管理及監督 •資源配置：人力資源及財務
作業面 Functional	•Work process design and documentation •Technical training •Control of process & service quality •Performance Measurement, analysis & evaluation	•工作流程設計及證明文件 •專業訓練 •控制流程及服務品質 •績效衡量、分析及評估

   (2) 飛航安全管理系統、航空保安管理系統及品質管理系統，這三個系統與多數系統由二面向組成不同，是由三個面向所構成：除了組織面、作業面，多了文化面(Cultural)；

組成要件分述如下：

a. 組織面，包含：

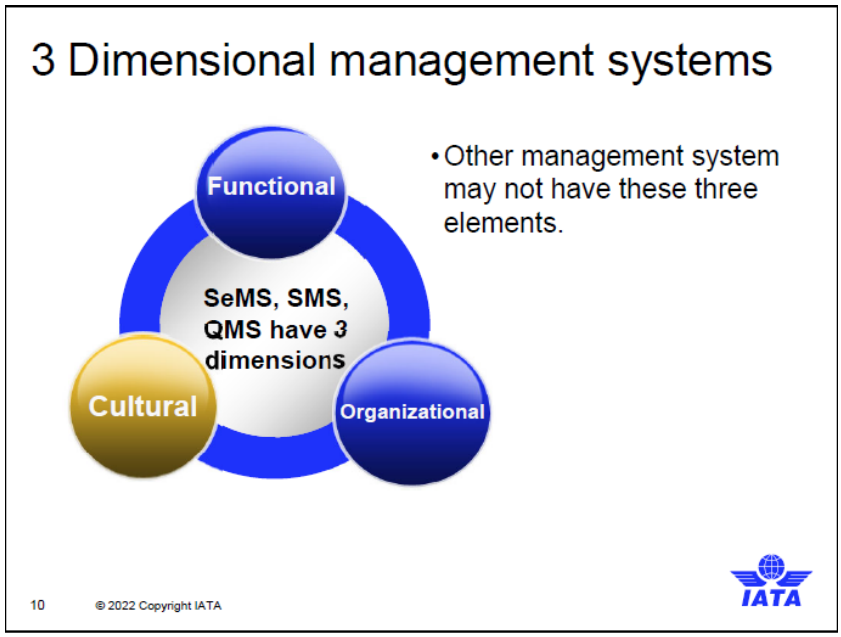
- 有一位最高負責人(Accountable Executive)，例如公司的 CEO 或 COO
- 航空保安負責主管(Head of Security)
- 支持的員工(Support Staff)
- 如果現行組織已經運行得很好，則無必要特別採用某個特定組織模型

b. 作業面，包含：

- 獨立的作業功能
- 支持公司運作
- 保安部門不是第一線作業單位，而是在日常作業中，透過監督作業管理保安

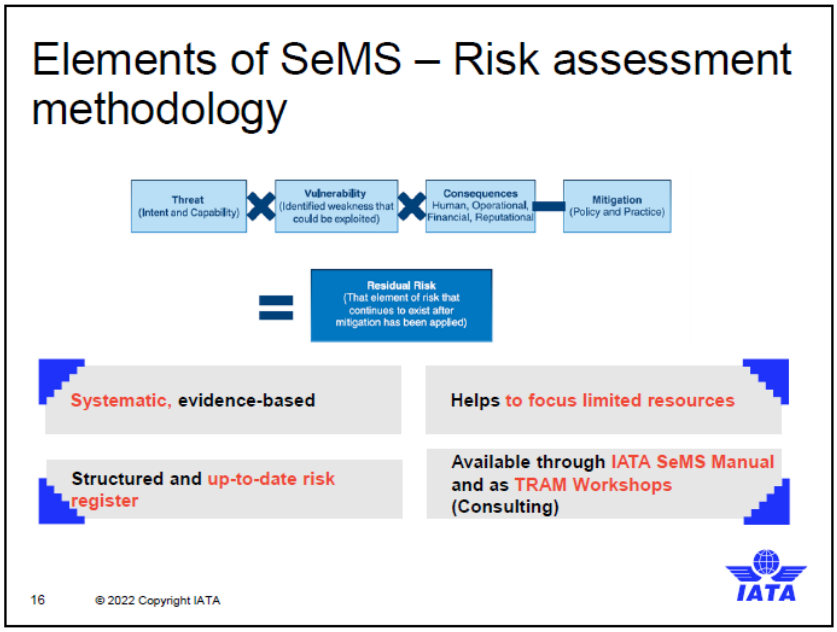
c. 文化面，包含：

- 每一個員工必須表現出健康的態度(Healthy Attitudes)、適當的行為(Appropriate Behaviour)，及自律/自我要求(Self-Discipline)
- 每一個員工必須瞭解最新保安威脅資訊，並對潛在的保安漏洞及非法干擾行為保持警覺
- 所謂文化，是有關「在這裡，事情是如何完成的」，包含不成文的常規、期待、明文規定等
- 面臨的挑戰是，如何說服企業保安是他們的責任。可透過下列方式達成：訓練及教育、持續精進及提升動機、將保安責任分配到企業內所有相關領域
- 文化的改變不可能一蹴可幾，必須隨著時間潛移默化
- 5 個保安文化下的子文化：Professor James Reason 所列出飛航安全管理系統的 5 個子文化概念，可同樣應用於保安上：自願報告文化、公正文化、學習文化、彈性文化、資訊分享文化



4. 主題三：航空保安管理系統的要素—風險評估作業

(1) 威脅(意圖及能力) x 脆弱點(經識別可能被有心人士利用之弱點) x 結果(人員、營運、經濟、名譽)-緩解措施(政策及演練)=殘餘風險(緩解措施實施後仍持續存在之風險)



(2) 實施航空保安管理系統的意涵：

a. 整合並涵蓋整個系統

b. 聚焦在最佳實務(Best Practices)，而非只是單純符合規定

c. 成效導向，而非硬性規定

d. 對於促進保安文化及提升航空保安有助益

(3) 如何執行航空保安管理系統：執行要件包含：政策、組織、推廣、風險管理(包含報告及調查機制)、監督查核/品質保證制度、計畫/手冊(規範及程序)

5. 小結：

(1) 人員是航空保安關鍵且必要的要素

(2) 高階主管必須為航空保安政策背書

(3) 瞭解在組織內發展及維持航空保安文化重要性

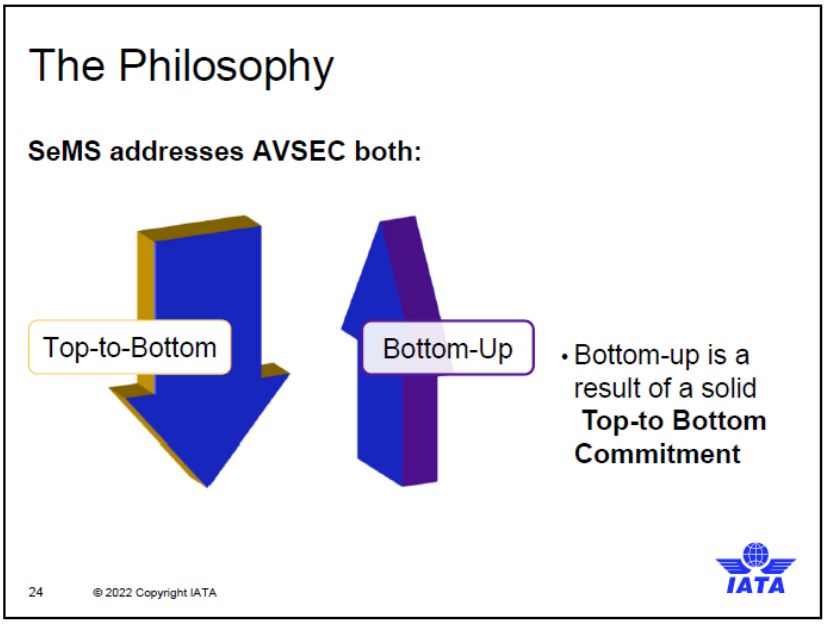
四、公司承諾 Corporate Commitment

1. 學習目標及主題(Learning objectives and topics)：

(1) 瞭解並說明如何運用保安政策，以形成高階主管之航空保安承諾

(2) 主題包含：高階主管的航空保安承諾、保安政策的重要性及介紹保安文化

2. 航空保安管理系統傳遞航空保安方式：同時包含由上至下(Top-to-Bottom)及由下到上(Bottom-Up)，其中由下到上的溝通，可反映由上至下堅實承諾的結果。



3. 航空保安政策(Company security policy)

(1) 是一套控制企業行為的機制

(2) 為了確保人員能以可預測、適當且對組織最有利的方式行動而存在

(3) 企業目標與航空保安目標必須相互連結

(4) 最基本的優先要務是取得高階主管的承諾，並且簽署航空保安政策聲明

4. 高階主管對航空保安承諾(Executive commitment to security)：

(1) 高階主管(Senior Management)：

a. 是航空保安的最高負責人

b. 負責奠定組織對於航空保安的態度

c. 發起組織航空保安文化

d. 負責訂定/核准可接受的航空保安標準

5. 航空保安政策必須符合以下要件：

(1) 與整體企業願景及任務保持一致

(2) 必須以白紙黑字，規範於航空保安計畫中

(3) 必須積極推廣

(4) 應動態調整：必須定期檢視及更新內容

6. 高階主管承諾之航空保安政策內容(經 CEO 核准且簽署背書)包含：

(1) 組織的核心價值

(2) 保安作業方法的基礎信念及核心要素

(3) 保安組織

(4) 符合規範並持續精進

(5) 自願報告機制及免責保障(No-Blame policy)

(6) 將保安的期待及目標清楚傳遞

7. 何謂保安文化：

(1) 能反映出真實的組織承諾(real Commitment)

(2) 代表態度(Attitude)，即人們認為保安的重要性

(3) 代表特性(Attribute)，即人們如何認知他們在保安扮演的角色

(4) 簡言之，就是人們在無人監督的情況下，自然呈現的狀態(How people behave when no one is watching!)

8. 文化的重要組成要素：

(1) 提供可取得的指引及程序

(2) 每一人員有清楚的職責

(3) 主管有效的支持及承諾

(4) 持續溝通及認知宣導

(5) 鼓勵自願報告(有效的回饋循環，Effective feedback loop)及持續挑戰

(6) 提供誘因，且實施文化慣例

(7) 高階主管的承諾

9. 如何測量保安文化：

(1) 沒有一個單獨或完美的文化，端看對於組織是否最有效

(2) 必須確保文化是彈性可因應需求調整，例如當威脅等級提高必須配合應變

(3) 測量的項目可能包含：

a. 員工是否覺得安全，是否認為保安高階主管是有效用的

b. 員工是否認為他們對於維護組織安全扮演重要角色

c. 員工是否遵守保安規範且正確行動

(4) 建議的測量工具包含：

a. 評估工具：訪談、討論/工作坊、問卷

b. 觀察事件報告的數量(增減情形)及內容

10. 小結：

(1) 人員是航空保安關鍵且不可或缺的要素

(2) 高階主管必須要為航空保安政策背書

(3) 瞭解發展及維持航空保安文化對於組織的重要性

11. 自我思考問題(self-directed task)：

(1) 組織內有多少部門

(2) 各部門是如何取得航空保安相關資訊

(3) 最近一次各部門詢問保安主管部門有關保安問題的時間為何

(4) 保安主管部門是如何與其他部門溝通

五、保安威脅和脆弱點評估 Security Threats and Vulnerabilities Assessment

1. 風險管理(Risk Assessment)

(1) 風險管理為定義、分析、評估及溝通風險以及接受、避免、轉移或控制風險至考量緩解行動之成本及效益後可接受之程度的過程。

(2) 風險管理的優點：

a. 增加達成組織目標之可能性。

b. 鼓勵積極主動的管理。

c. 符合法律及法規要求。

d. 提升通報機制。

e. 提升管理方式。

f. 提升利益相關者的信心及信任度。

g. 為決策和規劃建立可靠的基礎。

h. 改善控制方式。

i. 有效地分配及使用風險處理資源。

j. 提升作業之有效性和效率。

k. 提升損失預防及事件管理。

l. 最小化損失。

m. 提升組織彈性。

(3) 風險管理的原則：

a. 基於最佳可用的資訊。

b. 有系統、結構化且即時。

c. 敘述不確定性。

d. 創造價值。

e. 量身訂做。

f. 動態且反應變化。

g. 促進持續改進和增強

(4) 風險定義：

a. 風險：

-威脅或危險可能導致損害之可能性。

-可能的不良後果

b. 保安風險(Risk in security)：

-當與脆弱點(Vulnerability)，以及如果成功發生攻擊，可能會導致意外或預期的後果(Consequences)結合在一起時，等同於威脅(Threat)(SeMS 手冊第 4 版)。

c. 威脅(Threat)：

-意圖(Intent)和能力(Capability)因素的組合（一個人想要/不想做某事）（一個人有/沒有做某事的手段和工具）。

-將其置於更大的背景下，威脅是在指定時間範圍內對目標進行攻擊的可能性。

d. 威脅的可能性(Threat likelihood)：

-威脅的可能性取決於兩個因素的出現：攻擊特定目標(目標的吸引力)之意圖(慾望)及可以攻擊的能力。

-當兩個因素越高時，則可能性則越高，詳下圖(威脅評分表)

Overall Threat Levels and Likelihood

e.g. as advised by ICAO, State Authorities the Board of Directors or others

GRADE	LOW	MODERATE	HIGH	CRITICAL
More likely	3	5	7	8
Likely	2	4	6	
Less likely	1	3	5	

e. 確認威脅來源：

f. 威脅的特性：

-保安威脅與對手(adversary)有關。

-為協助定義威脅，我們需要處理下列議題：

-可能發生什麼?

-誰可能會做?

-他們如何做?

-他們什麼時候會做?

(5) 威脅評估：

a. IATA 威脅評估表

-以結構化方式紀錄威脅的工具。

-用來評估威脅是否可信。

-決定威脅等級(綠/黃/紅)。

-遵循 SeMS 手冊第 5.4 節說明有關操作威脅評估的決策樹方法。

b. 威脅評估

-幾乎無法影響威脅，但可以評估。

-威脅評估是對可能對民用航空產生不利影響的事件發生的可能性(likelihood)或概率(probability)的判斷。

-它的目的是決定：

-可信的威脅。

-它可能來自哪裡以及它可能如何被執行(perpetrated)。

-持續收集及評估情報、數據和資訊，以識別不斷變化的趨勢、現有和潛在威脅以及其他重大發展。

-戰略情報(strategic intelligence)定義意圖(intent)。

-戰術情報(tactic intelligence)定義能力(capability)。

-收集(Collection)、整理(Collation)、評估(Assessment)及發布(Dissemination)

-收集：使用所有可用的來源，隱蔽和公開的收集所有相關資訊和情報。

-整理：系統性排列相關材料並與所有其他相關情報進行比較。

-評估：判斷情報或資訊對國家資產的可能攻擊方面的重要性。

-發布：將評估結果發布給適當機關以確保其將威脅評估轉化為防範/預防措施。

c. 量化(Quantifying)來自恐怖組織的威脅

-領導能力(Leadership)：包括等級制度、合法政治代表的存在和魅力人格的使用。

-執行的實質性(Practicality of operation)：一個團體通過監視行動、獲取武器、發展資金來源和培訓特工來將理論目標（例如政治議程或宗教事業）轉化為實際應用的意願和手段。

-設施(Infrastructure)：結合例如小組單元的大小和數量、建立通信網絡、有效利用運輸及供應鏈等要素。

-人口(Population)：當地同情者支持網絡的存在，以提供避風港、食物和金錢--要麻出於對團體目標的同情，要麻出於恐懼和脅迫。

-戰鬥機制(Fighting mechanism)：被指派執行小組行動的人員的能力。這些組成員可以稱為戰士，例如劫機者，或技術人員，例如炸彈製造者。

-族群的存在(Presence of a group)

-攻擊歷史(History of attacks)

-內部衝突(Internal strife)

-經濟問題(Economic problem)

d. 威脅識別的資訊來源

-開放性來源

-內部報告(包含代理商)

-官方(如：國家產業資訊分享)

-航空專家或單位(產業與產業間資訊分享)

-國家情報組織-報告

-地區之站經理及員工

-大使館及區域保安官

-國際航空保安：熱點

-海外保安顧問委員會

-地區個人聯絡窗口

-每日情報彙整

-地區報紙

-風險管控族群

-媒體

(6) 脆弱點評估

a. 脆弱點定義：

-威脅及後果相互關聯的，為更好的解釋其關係，我們需要介紹脆弱點的概念。

-可以利用的弱點。因此增加了遭受攻擊時的暴露(exposure)和傷害。

-脆弱點：

-弱點有多廣為人知和瞭解。

-可以如何快速和輕鬆地利用這些...並且...這將引導思考被利用的後果。

-定義資產(Identifying the assets)→脆弱點

-旅客

-人員、組員及員工

-航空公司財產，包含航空器。

-航空站財產，包含航廈。

-與民用航空有關但非位於機場(Off-airport)之財產。

-導航設備

-智慧財產

-聲譽和商譽

-公司股票

-脆弱點識別

-對策(Counter measure)生產者

-監管者

-品質保證

-員工

-專家調查

b. 關鍵性(Criticality)

-重要的資產應於保安事件發生時，評估考慮下列事情：

-客戶/員工面臨的身體風險。

-一個架構的運營/經濟意義。

-對網格其他部分的影響。

-對恐怖份子/犯罪者的吸引力。

-資產的有效防禦等級。

c. 處理以識別之風險

-對策(Counter measure)可以是旨在降低已識別風險的行動、措施或設備。

-理論上，對策可以降低任何風險成分(威脅、脆弱點或後果)。

d. 緩解措施

Score	Definition of Mitigation Policy (e.g., documented standards and procedures)
1	**None:** There are no mitigation policies, measures, procedures, CONOPs or SOPs in place because no action has been taken and/or because no realistic and achievable measures are available (e.g., chemical attack).
0.75	**Limited:** Some areas and/or aspects are not currently covered by an existing policy or procedure. This includes aspects where policies or procedures may currently be in the design/delivery stage, but are not yet in place (e.g., chemical attack).
0.5	**Immature:** There is a broad policy in place for all areas and aspects, but it can be further developed and/or improved with additional guidance, CONOPs, SOPs, etc. (e.g., high risk cargo).
0.25	**Effective:** Policies and procedures that provide an effective level of mitigation are in place and fully documented (e.g., correct, complete and up-to-date SOPs and training requirements).

Score	Definition of Mitigation Practice (e.g., compliance with documented standards and procedures)
1	**None:** Documented mitigation policies and/or requirements are not implemented, actioned, adhered to and/or delivered at the operational level and/or there are no mitigating actions in place/adopted because no action has been taken to initiate activities and/or because no realistic and achievable practices are available (e.g., chemical attack).
0.75	**Limited:** Some areas and/or aspects of the documented policies/requirements are being enacted/delivered, but only partial implementation and/or level of compliance limits the level of mitigation being delivered. This includes aspects/activities where the company and/or individuals are attempting to deliver mitigation, but are failing due to a variety of reasons (e.g., poor training, lack of awareness, lack of supervision, lack of equipment, technology not provided/unavailable).
0.5	**Immature:** There is a broad level of compliance with and/or delivery of the policies/ requirements in place for all areas and aspects, but the quality/quantity of delivery can be or is in the process of being further developed and/or improved. This includes levels of compliance that could be improved via better advice, guidance, training and/or supervision as well as more efficient use of technology and/or resources. (e.g., refresher training is planned, recruitment is under way).
0.25	**Effective:** Effective mitigation is in place and is being consistently delivered to an acceptable standard (e.g., as determined by internal and external compliance/audit regimes).

(7) 後果評估

a. 後果定義：

-牛津字典定義後果為一個行動或狀況的結果或影響。

-為識別可能的結果，我們必須知道：

-什麼是可能的行動(威脅)。

-什麼可能被成為目標(脆弱點)。

-這些行動的後果是什麼(後果)。

b. 直接或間接後果

-後果通常可用四種方法測量：人類、經濟(財務)、運作或信譽，但可能也包含其他因素，例如：對環境的影響。

-恐怖攻擊的直接後果通常是攻擊背後的真正原因。

c. 評估可能的後果

-有必要定義/組合損失和脆弱點的影響評級。

-它可能因資產/設施而異。

-以航空站為例：對於空中交通管制塔臺來說，幾分鐘的停機時間可能會產生毀滅性的影響，而對於航空公司的售票處來說，同樣的停機時間只會產生輕微的影響。

d. 評級(Rating)後果

-毀滅性的(Devastating)：設施損壞/污染超出可使用範圍。大多數物品/資產都丟失、毀壞和損壞，無法修復或恢復。

-嚴重的(Severe) ：設施部分損壞/污染。部分物品/資產損壞或丟失，但設施大部分完好無損。

-明顯的(Noticeable)：設施暫時關閉或無法運行，但可以在不中斷超過一天的情況下繼續運行。

-輕微的(Minor)：設施對運營沒有重大影響。

Rating consequences – TRAM example

Table 5.3.3—Suggested Consequences Evaluation Scoring Chart

Impact	Human	Financial $(k?)	Operational	Reputational
8	200 + fatalities	1,000,000 +	Closure	Total loss
7	100 + fatalities	≤ 1,000,000	6 months +	International
6	50 + fatalities	≤ 100,000	3 months +	National
5	11–50 fatalities	≤ 10,000	1 month +	Regional +
4	11–50 casualties	≤ 1,000	1 Week +	Regional
3	1–10 fatalities	≤ 100	Days	Domestic
2	1–10 casualties	≤ 10	Hours	Local
1	No casualties	0	None	None

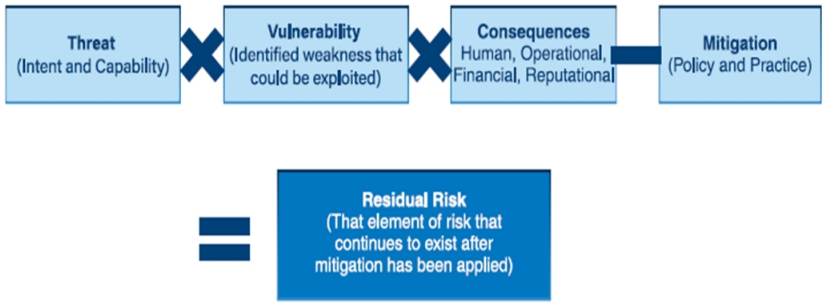
Source: IATA

(8) 風險定義

-字典對風險的定義為：

-風險(Risk, R)是一個事件的概率(Probability, P)或可能性(Likelihood)以及後果嚴重程度(Severity, S)的組合(Combination)(不是加總 Sum)。

-在保安，風險(Risk, R)可以被視為威脅(Threat, T)、脆弱點(Vulnerability, V)、後果(Consequences, C)及緩解措施的產物。



六、保安組織之建立 Building Security Organization

於建立有效之保安組織前(Security Organization)，首要應先明確組織保安職責分屬，再藉由組織內部之溝通及宣導，落實及優化組織保安文化：

1. 保安主管(Head of Security)之角色及任命

   保安主管為組織保安權責分署之樞紐，為建立有效保安組織，保安主管應具備一定之航空保安或航務知識，以有效進行組織部門保安權責分屬及組織保安之控管、維護及發展。此外，保安主管作為高級主管及組織間之溝通及組織各部門作業協調之媒介，亦應具備相應之授權。

2. 組織保安部門之角色及責任

   明確之部門結構及權責，作為組織保安中樞及內/外部協調單位，應具備資訊分析、組織彈性及應變能力，以裨益內/外部保安資訊之分派及消弭組織內部矛盾，且於組織發生緊急事件時，得有效進行處置。

3. 良好的溝通管道

   保安組織之基礎建立在明確功能角色定義及責任分屬，而為形成組織保安意識及鞏固組織保安文化，組織內部應建立持續溝通及宣導之管道，如：定期會議及宣導文宣，及建立正面的報告機制，以提供組織一線作業單位最新之保安知識，及塑造正面之報告文化，除得提升組織基層保安意識，亦使保安意識得融入至其日常作業中。

七、人力資源之遴選運用 Resource Management

航空保安為組織全體之責任，為有效落實組織保安，組織應招聘合適之人員，並以陪訓之方式，授予其相應職能，使其得以正確之方式完成對的工作；人員之招聘及培訓得依據以下原則執行：

1. 人員招聘

於招聘合適之人員時，組織得分為以下階段進行篩選：

(1) 藉由工作功能分析，釐清組織所需要之人員職能需求，如：所具備之知識、技能或經驗等。

(2) 瞭解組織是否具備相應因素得招聘到所需之人員，該因素分為「無法改變的因素」及「可能影響或改變的因素」，為招聘所需人員，組織得調整可變性因素，增加組織招聘競爭力。

a. 我們可能無法改變的因素：

- 工作性質(全職或兼職、輪班制)
- 工作地點
- 錄取所需的技能和能力(擬限制可用候選人)
- 與其他雇主的競爭

b. 我們可能影響或改變的因素：

- 工作誘因(是否具有聲望、社會地位等)
- 職涯機會
- 調職能力或技能
- 聲譽
- 金錢

2. 人員培訓

為使人員具備所需之知識及技能，並熟識其所要執行之工作，組織應依據工作職能所需，規劃相應之培訓計畫，以利人員得於有限的時間內具備所需職能。

因應 IOSA 及 ICAO 文件，於建立培訓計畫時，應考量以下：

(1) 初始訓練(Initial Training)

以理論為基礎授予受訓人員作業基本知識及瞭解相關作業風險，並利用實作進行模擬演練，使其理解實際作業狀況。

(2) 在職培訓(On-the-Job Training)

受訓人員於實際作業中，瞭解作業目的及熟悉標準作業流程，組織亦得於其中觀察受訓人員之適職性。

(3) 定期複訓(Recurrent and Requalification)

加強在職人員政策之熟悉性，並宣導及分享保安新知及國際趨勢。

(4) 測驗與評估(Testing and Evaluation)

組織得藉由測驗，瞭解受訓人員之學習成果，及評估訓練內容之有效性，並得依據評估結果進行調整，以增加訓練效益。

除考量上述建議外，組織亦應瞭解，毋論訓練種類，保安意識培訓(Security Awareness Training)應為必要之訓練項目，人員培訓除旨在使受訓人員熟知相關工作職能，亦在於培養人員作業之保安意識，通過訓練使作業人員知悉：

- 保安為每個人的責任。
- 每個人都應接受保安訓練。
- 每個人員於航空保安中扮演著什麼角色。
- 自身職責會對航空保安產生什麼影響。

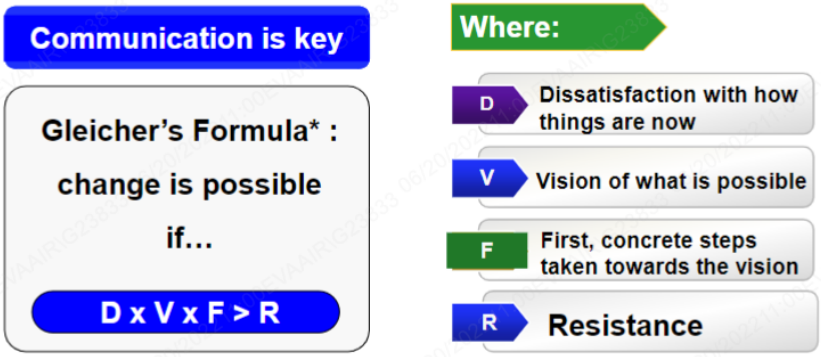
進以提升組織人員整體保安意識。

八、改變和專案管理 Change and Project Management

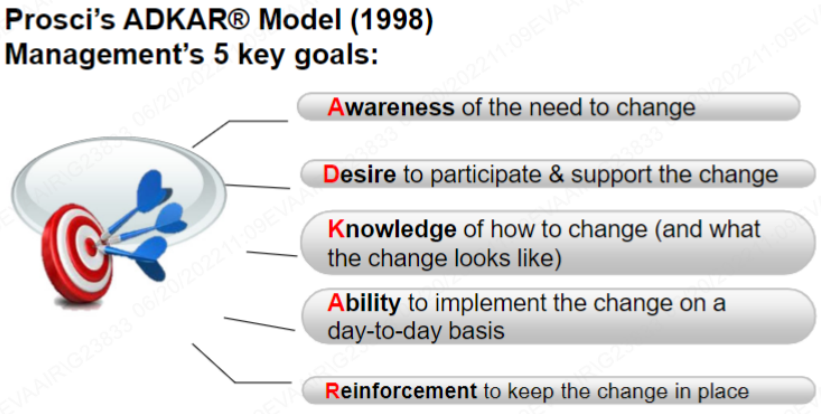
課程介紹 SeMS 航空保安管理系統於保安上，實施的過程中需要面臨及考慮的變革管理，不同的變革管理和策略及面對這些變革所需的技能。課程包括改變管理策略的流程、技能及策略從定義項目管理、識別、啟動、規劃、執行和控制到整個計畫的收尾，讓學員能充分了解面對管理計畫面臨變革時所具備的全面視野。

Why change management?為何改變管理策略?

基於人類學及心理學反映對於變革的人為趨勢，藉由說服員工改變既定的流程以提高生產力，促使個人及組織長期的工作效率進而解決問題。透過每次的管理革新提高對於每一位員工對改變的可信，以更明智的決策和判斷來達到更有效的運作，並透過資源分配和衡量預期的結果。



透過 Gleicher's formula 如果改變是可能的可以透過 D(對現狀的不滿) x V(可能的願景) x F(具體的步驟) >R(抵抗)，就有機會做出改變。

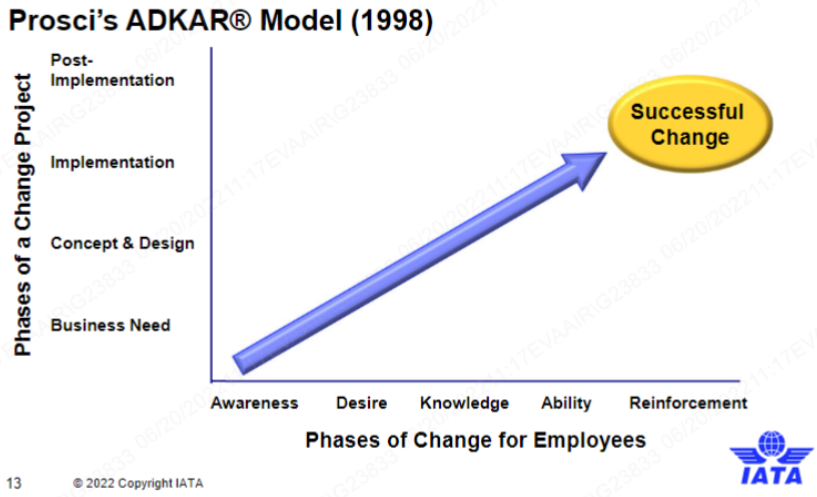


管理流程的改變基於 1998 年 Prosci's ADKAR Model 共有 5 個目標

1. Awareness:意識到改變的需求

2. Desire:渴望參與和支持改變
3. Knowledge:知道如何改變及改變成甚麼樣子
4. Ability:有能力實行改變
5. Reinforcement:致力於持續改變

經過 5 個關鍵目標實施並透過執行可達到成功的改變。



另外透過 Kotter's 8 階段的策略連結可以實施監督各階段改變的進程

1. Establish a sense of urgency(建立緊張感/迫感)
2. Creating a guiding coalition(建立指導聯盟)
3. Developing a vision & strategy(制定願景和策略)
4. Communicating the change vision(傳達變革的願景)
5. Empowering employees for broad based action(傳授員工採取廣泛的行動)
6. Generating short term wins(產生短期的成功)
7. Consolidating gains and producing more change(鞏固勝利的成果並製造更多變化)
8. Anchoring new approaches in the culture(在新的文化中錨定新方法)

Change Management Skill & Strategy

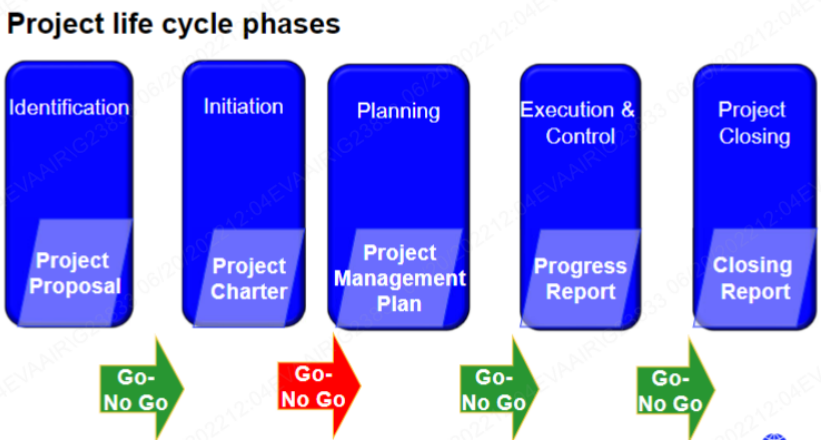
管理規則改變的技巧和策略，我們將透過 4 種不同的技巧來促進計畫的改變，Political skills、Analytical skills、Business skills、Communication/

relationship skills，經過管理單位的技巧來溝通各單位進行，由 **Empirical-Rational** 經驗及關係

的傳承提供激勵措施，**Normative-Re-educative** 規範及重新教育，使員工遵守文化規範和價值並基於管理規則重新定義和重新檢視來溝通發展，**Power-Coercive** 人通常是基於合規僅做他們想做的事情此時就必須透過權力行使和強加制裁來做出改變，**Environmental-Adaptive** 人們常反對損失和破壞，但他們很容易適應新的情況，變革是建立在新組織的基礎上並將人從舊的制度轉移到新的上，經過個技巧及策略對組織內的員工進行溝通來促成管理策略的改變。

Defining Project Management

將知識技能、工具、技術用於專案活動以滿足利益交換者的期望，進一步可以透過按時或按預算的甘特圖，將可能分散的人力對重要因素重新獲得分配。一個專案經理的職責，將制定的目標在現在範圍內及時限內完成目標，有效的整合所有資源並做出決定，於發生衝突時有效解決並作為工通樞紐最後與所有利害關係者進行談判。



Project Execution & Closing

專案執行到結案，整個專案的過程透過核心組織召開常態性的會議，並按照時辰評估進度:包含整個計畫潛在的延遲、緩解的計畫、轉移或分配額外的資源、評估造成的影響及準確的評估預測。結案時將整個產品交付範圍包括•Measure client satisfaction 衡量客戶滿意度• Post project service, training 項目後期服務、培訓• Project evaluation 項目評估• Risk review 風險審查• Reassignment 重新分配• Contract closing 合同關閉• Archiving project documentation 歸檔項目文檔，由上述內容來傳承後進行項目結案。

九、保安風險管理 Security Risk Management

本章節介紹如何進行航空保安的風險評估，風險評估的過程包含 5 個大步驟，並定義何謂航空包安內的風險，如何計算風險，簡介航空保安的網路安全並如何實行網路保安的風險評估。

Figure 5.3.1—The Risk Management Process

Step 1 : Communication and Consultation:與內外部利害關係人協商應在風險評估過程中所有階段進行。

Step 2 : Establishing the Context:闡明目標並定義要考慮的內外部參數，並設定範圍和風險標準。

Step 3 : Identifying the Risks and Possible Target Areas:定義風險和可能的目標領域的綜合清單，預想可能會影響甚麼，可能在何時何地觀察到影響，為甚麼會發生以及如何發生?

Step 4 : Analyzing the Risks:著眼於漏洞，確保這些漏洞被得知利用的速度能於發現問題前得到解決

Step 5 : Evaluating the Residual Risk and Setting Priorities:此階段旨在對風險進行優先排序並協助決定處理風險的順序。

Step 6 : Treating the Residual Risk:確定緩解的方法已將風險水平控制在可接受的水平。

Step 7 : Monitoring and Review:返回 step1 並不斷重新檢視並監控整個風險事項。

為清楚明確定義風險為何，將透過名詞解釋定義風險 Risk(R)，在字典裡風險是一個”組合”而不是總和的概念，風險是由 R=P x S，風險為事件的概率乘以一個事件和其後果的嚴重性 S 相乘後得出 Risk 值。然在安全方面，風險可以看做是威脅(T)的產物加乘漏洞及後果減去緩解措施 R=T x V x C-M 所產生的值。

以上述定義來檢視航空保安的風險有

1. Bomb threats (including ‘dirty’ ones)炸彈威脅
2. Contamination of catering 航餐汙染
3. Destruction or damage to aircraft 飛機毀壞及損壞
4. In flight security incidents involving crew and passengers 涉及機組人員和乘客的飛行安全事件
5. Theft of passenger baggage, freight and mail 盜竊旅客行李、貨物、郵件
6. Interference with air navigation facilities 干擾空中航行設施
7. Extortion involving threats to aircraft 涉及威脅飛機的敲詐勒索
8. Airport sabotage/attack 機場破壞或攻擊
9. Hijacking 劫機

新興的航空保安風險:網路保安

由美國國家標準與技術研究院(NIST)定義網路保安:為防止損壞、保護和恢復電腦電子通信系統、通信服務、有限通信和電子通信，包括信息其中的可用性、完整性、身分驗證、保密性和不可否認性。當今的網路商業生態系統需要轉變，從側重於預防和控制的安全到風險評估，優先考慮公司及組織最有價值的資產及最相關的威脅，整個網路保安的風險評估與防護應該是一個持續性的過程，對新的 IT 系統及部門進行風險評估，衡量所有資訊網路事件對航

空網路保安可能造成的影響。

可透過威脅和風險審計矩陣進行輔助，從 SeMS 的手冊所提供的資訊，實體識別、計算和監控航空保安的風險，藉由策略、運營來使其風險評估的決策和證具有確定緩解風險的優先順序。

十、事件報告和人為因素 Occurrences Reporting and Human Factor

在大部分的航空保安作業中，相關人員都會需要操作各式軟硬體。這時確保人機介面操作順遂就至關重要，不只要軟硬體設備作動完好，操作設備的人員更是最關鍵的，也是最複雜、潛在的最薄弱的環節。而人為因素探討的就是人與周遭環境的連結，找出其限制，想辦法降低事件發生可能性，降低後果嚴重性，並提升效率，以求更順遂安全的作業。

透過訂立明確的安全規範，將人為因素納入軟硬體設計的考量中，確立標準程序以提高應變能力，並設定選才、訓練、考核和績效管理的標準，都可最大程度的降低人為因素導致的意外發生。在航空保安方面，探討人為因素的風險，就要考量「動機、能力及資源」三個層面。動機又與對工作的滿意度息息相關，在 Herzberg 的理論中，為了提升動機，首先要消除對工作的不滿，例如修改糟糕且阻礙發展的公司政策、提供有效的監督、建立尊重的文化、提供工作安全保障等；再來，要提高對工作的滿意度，可以從與作業相關的激勵面去設想，想辦法讓工作充實具有意義，例如提供成功的機會，認可員工的貢獻，創造有回報的工作，提供晉升機會、培訓或發展機會等。人員的能力則可能導致技術失誤、決策失誤或知識缺發而致的失誤。資源管理或疏失管理的介入則可減少失誤的產生並預防再發生。以 SHEL 模型輔助，可有效找出人與硬體、環境、軟體的介面，用以改善程序、設備或作業模式。另外，保安文化也同樣會影響人為因素，正向的保安文化可提升保安意識及風險管理的有效性。而事件報告所帶來的數據可支持前述人為因素的探討，且事件報告不僅止於提報，其流程應涵蓋分析、調查及宣導，以此持續的提升安全。

十一、 案例研究 Case Study

談航空保安文化的建立，911 後的美國聯合航空所建立的架構絕對是一個絕佳 範例。自 911 攻擊事件後，首先，聯合航空建立了全員通報的機制，鼓勵員工 反應保安疑慮、漏洞；另設立全年無休的保安服務專線，及時接收員工的問題 並告知後續處置措施，並藉由公司高層當責的管理態度處理保安問題，使工作 環境更加安全無虞。隨後，提倡機敏文件傳遞的規範，進而再探討網路保安等 議題，此番環環相扣的政策與程序建立，為的就是倡導並推廣航空保安文化， 將航空保安認知深植於所有員工的意識。航空保安的每一個案件均有其獨特 性，卻又有著以造成重大人員傷亡的相同目的性；如何防止航空保安事件的發 生是航空相關單位持續的課題。

十二、 緊急情況、事件管理及應變計畫 Emergency, Incident Management and Contingency Planning

緊急事故管理內容提及為何需要危機管理、危機管理的目標、調查與報告保安事件的重要、危機管理計畫的不同階段、網路保安事件、危機管理不同的組成內容與如何設計危機管理、危機管控區域、緊急應變中心(EOC)及危機管理小組等。

十三、 保安品質管制 Security Quality Control

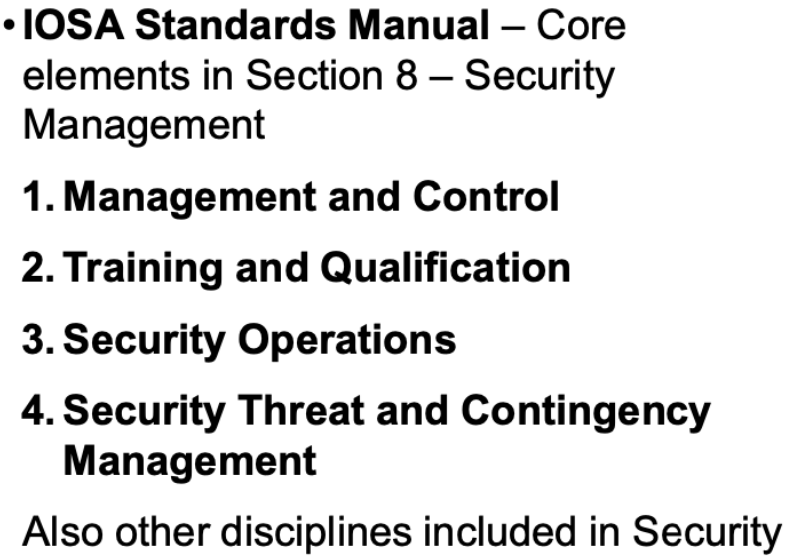
保安品質管制內容提及品質管制的重要性、介紹不同工具以提高品質管制的效率、解釋不同的方法和工作以促進品質管制；另說明 PDCA（Plan-Do-Check-Act）循環式品質管理，針對品質工作按規劃、執行、查核與行動來進行活動，以確保可靠度目標之達成，以促使品質持續改善，由美國學者愛德華茲·戴明提出，也稱戴明環。

十四、 IOSA

針對任何一項作業系統，每當需要檢視作業是否落實執行時，查核總是一項必不可少的方式，如同 IATA 制定了各項作業標準，但要如何去確認執行的落實與否，因此便有 IOSA 這項國際統一查核及評估作業的需求，且因為 IOSA 為國際查核的標準，因此若航空公司有相關的

作業，便可提升安全的層級，也因為是一治性的標準，可減少航空業界內互相查核的次數，畢竟已經由國際認證的公司來執行，代表公司內的相關作業也都符合國際上要求。

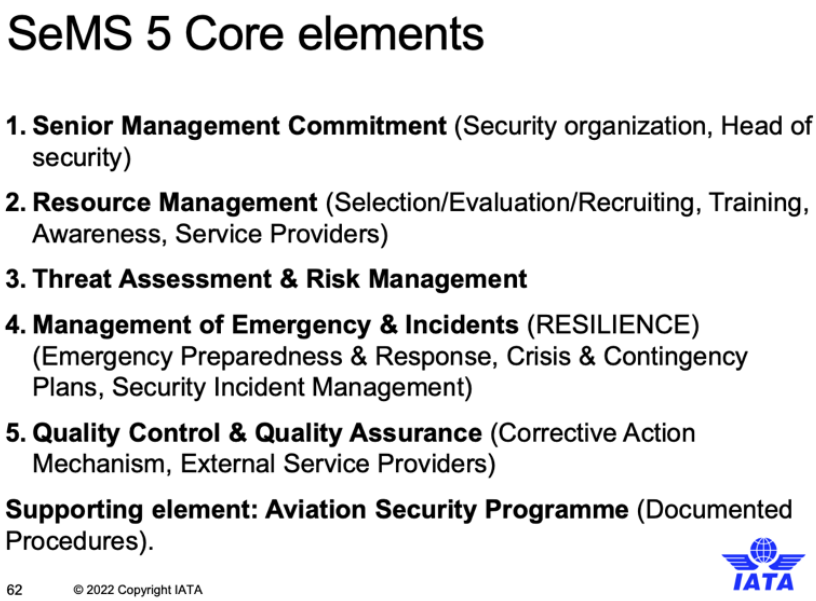
課程中先介紹 IOSA 整個查核的歷史演變、查核範圍及查核標準，而後帶到第 8 章保安的相關查核內容，主要分為管理及保安控制、訓練及資格、保安相關作業及保安威脅及緊急應變計畫。



而後續講師僅簡單介紹查核內容中的內容但並無多做解釋，因為以上項目其實都是國際規範或條約中必須執行的項目，且講師亦認為當需要執行 IOSA 時皆會有更近一步了解，課程中僅讓學員了解這項作業的目的。

十五、 SeMS 實施 & 結訓 SeMS Implementation & course close

在課程最終的部分，講師則引導大家思考 SeMS 的改善作業，由規範、改善方式及最重要的五項核心元素，來讓大家重新思考如何可更有效的改善管理系統，並且將前幾日授課後累積的作業問題，由打在簡報內的方式，現場讓大家將想法作為討論。



肆、 心得與建議

在課程開始前，講師就詢問所有學員對於本課程的期待是什麼。有人希望全面了解 SeMS 的理念；有人希望針對 SeMS 的細項進行研討，瞭解如何建立及推廣組織的根本-保安文化；有人希望瞭解針對不同規模及作業的組織，SeMS 的具體作為有哪些。

課程中透過一個完整的案例研討－談討美國聯合航空保安文化，理解到公司管理高層承諾航空保安的重要性，有更多深刻的瞭解。保安組織的建立及文化的形成，最主要的不吝為管理階級之支持，上行下效進而形成基層向上之自發性作為，惟如何形成基層自發性文化，為多數組織遭遇之困難點。倘若欲促進基層向上之自發性文化，除前述管理階級之支持外，應增加具體措施，以顯示組織對於保安文化之支持及看重，並藉此累積管理階級對基層人員之信任度。高級主管之支持多為政策性佈達，如：提倡正義文化等，而倡導性之宣導方式多難以深入基層保安意識，時常淪為政策性口號，故若組織增加具體措施，如：提供獎勵等，除得提升基層人員保安意識，亦可促進組織保安文化之推廣。

講師還提及航空安全系統 SMS 與航空保安管理系統 SeMS 概念相似，並帶領研討許多可能導致 SeMS 推動不成功之議題，例如：公司/組織高層不重視、沒有經費、沒有有效溝通管道、回饋機制不健全、員工意識不足等，學員皆能理解，惟部分原因非學員層級能夠改善。探討

根本原因為國際民航組織針對 SMS 及 SeMS 規範篇幅及力度不同（SMS 有 19 號附約及 Doc.9859 支持，且為各國必須推動項目；SeMS 只在 Doc.8973 內一個章節簡述，且非各國比須推動項目），導致各國或相關單位於推動時對兩者之重視程度不同，另亦因 SeMS 國際間可參考文件較少，普遍航空保安相關人員較無法全盤瞭解推動概念及方法，再者航空保安情資及資訊多屬密件，於風險管理之情資、資料來源收集部分相較 SMS 困難，爰 SeMS 推動尚有待整體航空產業努力。

另外，課間學員提問有關航空保安是否有像近期危險物品建立以能力為基礎之訓練與評估機制，以及網路保安講師能量應如何建立（保安及資訊人員互不瞭解彼此專業）。講師回應目前據他瞭解，航空保安尚未對於前述訓練機制有具體或明確規範。另有關資訊人員與保安人員在網路保安的訓練角色，講師表示他認為組織內不可能會有太多新的部門（例如聘請新的通才），以現有的部門分工來講，考量保安未來會牽涉到越來越多資訊化系統，且為了人員本身能力加值，建議保安專業人員應該要主動瞭解網路保安。

本次課程讓所有學員對 SeMS 有了通盤的理解，瞭解航空保安管理系統(SeMS)的內涵、組成及操作方式，而講師藉由提舉自身經驗、課間演練及互動交流，使學員能更容易將理論面融入至實踐應用。尤其藉由講師主持學員針對課間三道議題的集體討論，透過各自把意見寫在電子白板上分享彼此的經驗並腦力激盪，再加上講師的意見整合及經驗分享，更能學習到許多不同的觀點，理解國際對於 SeMS 的推動及相關做法。不論課間或課後，講師也提供很多國際的網站連結資源讓大家能夠線上參考，並於午休時間留有充分的討論時間，盡力輔導並回答學員的疑問。

惟原先預想課程會學習到平時較不熟悉的實務操作部分，例如績效指標訂定、風險評估作業執行等；並可針對規模較小，作業較單純的航空公司，得到適性適所的 SeMS 啟發。但因本次課程係側重於基礎理論講授，而實務作業或案例經驗分享等略顯匱乏，是未來希望能夠再更持續瞭解及精進的部分。實際如何在航空公司或組織中施行仍須研究或有相關實施經驗者帶領，方能實施順遂。

而本次課程採視訊方式實施，有需多意料之外的好處，例如課程教材為電子檔，非常有利於

事先預習及課後查找資料，有助於快速理解課堂內容，並可於課後更有效的轉化教材資源；且靠著視訊軟體優秀的即時回饋功能，學員可直接於課程畫面上註記圖樣或文字，以簡短文字溝通取代每個人口頭自我介紹或逐一回覆，除大幅減省課程時間及口頭回應壓力，也補足實體課程互動部分，亦可幫助講師確認學員的專注及理解程度。另外相較於實體課程，多了很多可查詢資料及做筆記的時間，更能專注於課程本身，對於課程內容能夠更即時且深入瞭解。

很可惜的因為新冠肺炎疫情影響，無法與講師學員面對面現場互動。雖然視訊教學的確消弭了距離的障礙，且與講師的一對一互動影響不大，但學員間的交流卻幾乎不存在，少了業界交流的這一環，著實是個遺憾。

伍、 附錄

結業證書

This is a secured QR-code
To verify it, please refer to
www.iata.org/training-authenticate

Certificate

This is to certify that

Tzu-Yu Kuo

born on 04 November, has passed with distinction the IATA LIVE virtual classroom course

Security Management Systems - SeMS - Virtual Classroom

23-26 May 2022

given by instructor(s) Stephen Ackroyd

Willie Walsh
Director General, IATA

0001368615 YAS

This is a secured QR-code
To verify it, please refer to
www.iata.org/training-authenticate

Certificate

This is to certify that

Mei-Chen Chiu

born on 30 May, has passed with distinction the IATA LIVE virtual classroom course

Security Management Systems - SeMS - Virtual Classroom

23-26 May 2022

given by instructor(s) Stephen Ackroyd

Willie Walsh
Director General, IATA

0001374425 YAS

Certificate

This is to certify that

Yuan Chan

born on 09 October, has passed with distinction the IATA LIVE virtual classroom course

Security Management Systems - SeMS - Virtual Classroom

23-26 May 2022

given by instructor(s) Stephen Ackroyd

Willie Walsh
Director General, IATA

0001374452 YAS

Training

This is a secured QR-code
To verify it, please refer to
www.iata.org/training-authenticate

Certificate

This is to certify that

Lin Wei-Ting

born on 15 May, has passed with distinction the IATA LIVE virtual classroom course

Security Management Systems - SeMS - Virtual Classroom

23-26 May 2022

given by instructor(s) Stephen Ackroyd

Willie Walsh
Director General, IATA

0001368610 YAS

Training

This is a secured QR-code
To verify it, please refer to
www.iata.org/training-authenticate

Certificate

This is a secured QR-code
To verify it, please refer to
www.iata.org/training-authenticate

This is to certify that

Kuei-Lin Wu

born on 21 October, has passed with distinction the IATA LIVE virtual classroom course

Security Management Systems - SeMS - Virtual Classroom

23-26 May 2022

given by instructor(s) Stephen Ackroyd

Willie Walsh
Director General, IATA

0001376016 YAS

Training

Certificate

This is a secured QR-code
To verify it, please refer to
www.iata.org/training-authenticate

This is to certify that

Chieh Yin

born on 25 April, has passed with distinction the IATA LIVE virtual classroom course

Security Management Systems - SeMS - Virtual Classroom

23-26 May 2022

given by instructor(s) Stephen Ackroyd

Willie Walsh
Director General, IATA

0001368665 YAS

Training