出國報告（出國類別：訓練）

參加國際空運協會（IATA）舉辦之「航空網路保安（Aviation Cyber Security）」課程報告

服務機關：交通部民用航空局

姓名職稱：覃皓儀 技士

派赴國家/地區：瑞士/日內瓦

出國期間：114 年 9 月 6 日至 14 日

報告日期：114 年 10 月 2 日

提要表

<table>
<tr><td>系統識別號：</td><td>C11401718</td></tr>
<tr><td>視訊辦理：</td><td>否</td></tr>
<tr><td>相關專案：</td><td>無</td></tr>
<tr><td>計畫名稱：</td><td>航空保安檢查員訓練</td></tr>
<tr><td>報告名稱：</td><td>參加國際空運協會（IATA）舉辦之「航空網路保安（Aviation Cyber Security)」課程報告</td></tr>
<tr><td>計畫主辦機關：</td><td>交通部民用航空局</td></tr>
<tr><td>出國人員：</td><td>
<table>
<tr><th>姓名</th><th>服務機關</th><th>服務單位</th><th>職稱</th><th>官職等</th><th>E-MAIL 信箱</th></tr>
<tr><td>覃皓儀</td><td>交通部民用航空局</td><td></td><td>技士</td><td>薦任(派)</td><td>聯絡人：
aj2992@mail.caa.gov.tw</td></tr>
</table>
</td></tr>
<tr><td>前往地區：</td><td>瑞士</td></tr>
<tr><td>參訪機關：</td><td>無</td></tr>
<tr><td>出國類別：</td><td>訓練</td></tr>
<tr><td>出國期間：</td><td>民國 114 年 9 月 6 日 至 民國 114 年 9 月 14 日</td></tr>
<tr><td>報告日期：</td><td>民國 114 年 10 月 2 日</td></tr>
<tr><td>關鍵詞：</td><td>航空網路保安</td></tr>
<tr><td>報告書頁數：</td><td>29 頁</td></tr>
<tr><td>報告內容摘要：</td><td>本次航空網路保安訓練課程，聚焦航空產業數位化所面臨的威脅與挑戰，結合國際法規標準、各類網路攻擊案例、系統風險評估、威脅因應及資訊安全管理系統（ISMS）等部分進行探討，課程亦涵蓋威脅辨識、風險矩陣分析、企業資安治理等重點，並透過實務模擬強化學員在網路保安管理、風險評估及事件應變方面等專業能力。</td></tr>
<tr><td>電子全文檔：</td><td></td></tr>
<tr><td>附件檔：</td><td></td></tr>
<tr><td>限閱與否：</td><td>否</td></tr>
<tr><td>專責人員姓名：</td><td>劉哲妤</td></tr>
<tr><td>專責人員電話：</td><td>02-23496193</td></tr>
</table>

摘要

本次航空網路保安訓練課程，對於航空產業數位化發展所面臨的威脅與挑戰，結合國際民用航空組織（ICAO）《國際民航公約》第 17 號附約、資安法規與標準，並融入國泰航空資料外洩、波蘭航空 DDoS 攻擊、曼谷航空勒索軟體事件等真實案例研討，協助學員理解航空網路攻擊的手法、動機與潛在影響。課程深入探討 CIA 三要素（機密性、完整性、可用性）、風險評估模型、威脅情境分析、事件回應生命週期（從準備、偵測與分析、控制修復、事後分析）、企業資安治理架構以及供應鏈風險管理機制，並結合資訊安全管理系統（ISMS）的建置、運作與持續改進，提供系統化的資安管理思維。

課程透過分組討論、情境模擬，提供學員演練威脅辨識與風險矩陣分析技巧、事件應變等，培養學員了解航空網路保安核心概念。

目次

壹、目的

隨著全球航空產業轉型數位化，先進資訊與通訊技術 ICT（Information and Communication Technology）之導入已成為提升飛航安全、運行效率及經濟效益的重要推手。然而，數位化所帶來的便利與效益亦伴隨日益嚴峻的網路威脅與資安風險。國際民用航空組織（International Civil Aviation Organization，ICAO）於《國際民航公約》第 17 號附約 2018 年修訂版中，已明確將航空網路保安納入規範，要求各國主管機關及航空業者辨識關鍵資訊與通訊系統，採取適當防護措施，以防範非法干擾行為，確保航空運輸體系之安全與韌性。

近年實際案例顯示，駭客攻擊目標已從傳統資訊系統延伸至航機通訊系統、機場營運設施、供應鏈網路與旅客個資平台等，攻擊手法亦趨於專業化與多樣化，包含惡意軟體滲透、勒索攻擊、分散式阻斷服務(Distributed Denial of Service，DDoS)、全球導航衛星系統(Global Navigation Satellite System，GNSS)干擾與訊號欺騙等，對飛航安全、營運、資料保密性及品牌造成潛在衝擊，在此情況下，我國航空保安檢查員於執行查核、檢查及測試作業時，亦需具備航空網路保安專業知識與風險評估能力，俾能有效確認各航空站與航空公司之網路保安措施是否符合國際標準及國內相關法規要求，以防範網路威脅。

透過參與本次航空網路保安課程，檢查員可系統性學習國際標準、熟悉威脅辨識、風險矩陣分析、事件回應及持續改進機制，並瞭解資安管理系統（Information Security Management System，ISMS）於航空營運之應用，藉由強化檢查員之專業職能，期能全面提升我國航空網路保安防護能量，確保飛航安全與產業永續發展。

貳、課程概要

一、課程名稱：航空網路保安（Aviation Cyber Security）

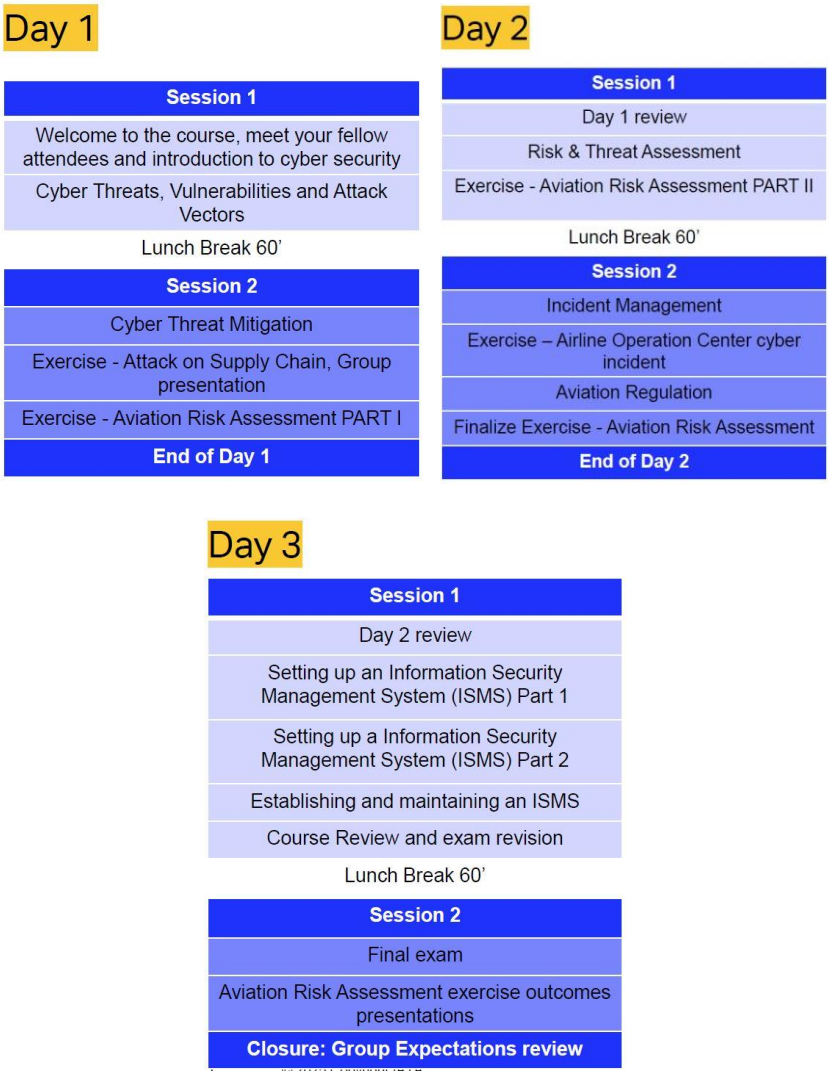
二、課程日期：114 年 9 月 10 日至 12 日

三、上課地點：國際航空運輸協會日內瓦訓練中心

（IATA Training Center — Geneva）

四、課程規劃：本課程共 24 小時，含 1 次測驗、3 次隨堂分組報告及 1 次專題分組報告。

五、參訓學員：本次課程除我方人員外，尚有來自瑞士、德國、奈及利亞之學員參與。



圖：本次訓練之課程大綱

Performance Assessment & Grading

- **Final Exam**

  50%
- **Presentation** (of the group exercise)

  30%
- **Participation**

  20%

10

圖：課程評分標準

圖：國際航空運輸協會日內瓦訓練中心

參、課程內容及訓練目標

本次訓練課程，主要包含航空網路保安之基本概念、網路威脅之因應、風險評估與事件管理及資訊安全管理系統（ISMS）之建立，學員完成課程後應能夠：

一、瞭解航空網路安全威脅

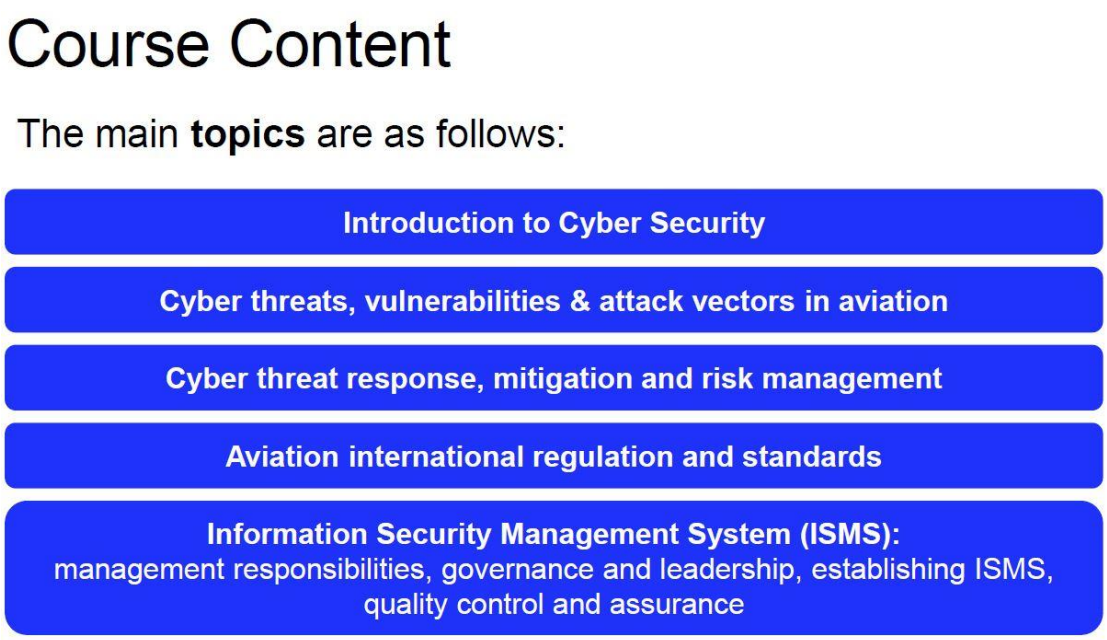
二、提出風險緩解建議

三、說明風險評估的主要步驟

四、排定航空服務網路風險順序及等級

五、理解航空網路安全法規的演變與未來要求

六、建立並定義有效的航空網路安全企業架構



圖：課程主要議題

一、 網路保安介紹

(一)資訊保護的核心原則(資安三要素)（CIA Triad）：

網路保安可視為一套保護措施，意旨在全面防護重要資料（如客戶資料、財務細節、知識產權等）以及保護提供資料存取運作的基礎設施等（包括硬體設備、應用軟體和網路連線）免受惡意攻擊。

儘管各國際企業如：國際標準化組織（International Organization for Standardization，ISO)、美國國家標準技術研究院(National Institute of Standards and Technology，NIST)、國際電信聯盟(International Telegraph Union，ITU)對於網路保安的定義略有不同，但其核心精神都圍繞著保障資訊的三大基本原則，即著名的 CIA 資安三要素(以航空業為例)：

要素名稱	核心定義	簡要說明	遭受破壞的後果
機密性 (Confidentiality)	避免數據洩露	確保資訊只有授權人員能取得	敏感資訊洩露、乘客資料外洩、商業機密被盜
完整性 (Integrity)	確保數據準確	防止資訊遭到非法的竄改或破壞	飛行數據被竄改、航班時刻表錯誤、財務報表不準確
可用性 (Availability)	確保服務不中斷	確保系統和數據在需要時能夠隨時存取	系統癱瘓、航班延誤或取消、機場運作中斷

圖：CIA 資安三要素

換言之，有效的網路安全，應於機密性、完整性與可用性之間取得適當平衡；而航空網路保安亦遵循此原則，並強調人員與技術資源之整合與協調，在考量網路安全時，可以 CIA 資安三要素原則進行評估及決策的關鍵，以確保航空公司網路安全，以下就 CIA 資安三要素進一步討論及說明：

1、 機密性 (Confidentiality)：確保資訊只被授權的人員、實體或系統存取，如：

(1) 乘客身分資訊：姓名、護照號碼、常客資料。

(2) 商業敏感資訊：航班排程、票價策略、營運成本。

(3) 國家/軍事資訊：國家安全和防禦機密數據。

2、 完整性 (Integrity)：確保資訊和資訊處理，非經未授權人員非法竄改或破壞，如：

(1) 飛行數據：確保機組人員或自動駕駛系統獲取之導航資料、氣象數據或飛行計劃正確無誤。

(2) 維護紀錄：確保飛機維護和零件紀錄未被竄改。

(3) 系統配置：確保航空系統軟體和硬體配置保持於安全操作狀態。

3、 可用性 (Availability)：確保被授權使用者在需要時能存取資訊或資源，如：

(1) 航空管制系統：確保航管系統正常運作，以維持空中交通的順暢和安全。

(2) 航班運作和旅客服務系統：登機、行李處理、通信等系統必須正常提供服務。

二、 航空網路威脅

(一)網路威脅（Cyber Threat）：

1、 定義：發生未經授權的存取、破壞、洩露、竄改資訊或中斷服務等事件或事故，或產生之後果對於國家、個人或企業之營運與資產造成不利影響，均屬於此範疇。

2、 說明：網路威脅來源具有多樣性，不同的威脅者(Cyber Threat Actors)懷有各種動機，這些動機可能包括：受利益驅使的網路犯罪集團、受國家支持的駭客、具有社會或政治議題主張的駭客行動主義者，以及擁有內部存取權限的內部威脅，不同的威脅者以多種方式利用系統弱點，以達成其經濟、政治或破壞目的。

(二)網路威脅者（Cyber Threat Actors）類型：

1、 國家級攻擊者（Nation State Actors）：受政府資助，主要目標在於獲取具競爭性的資訊與資源，通常於間諜活動、破壞行為及智慧財產竊取。

2、 網路犯罪分子（Cyber Criminals）：此類威脅者活動範圍較廣，其主要動機在於追求利益，威脅者常透過竊取個人資訊，例如出生日期、護照資料等，其不僅可入侵個人資料，亦可能將資料轉售給其他犯罪分子。

3、 激進駭客（Activists）：駭客行動主義者，其動機可能來自財務利

益，通常因某種理念而發動駭客行為，例如環保議題。

4、 恐怖分子（Terrorists）：透過破壞網路以取得控制權，或摧毀他國能力與運作，如支持「伊斯蘭國」（ISIS）的駭客曾發動之網站攻擊，並於受攻擊網站出現「網路聖戰」的字樣。

5、 尋求刺激駭客（Thrill-Seeker Hackers）：攻擊技術較低的駭客，其通常依賴現成工具進行攻擊，多半以娛樂或獲得關注為動機，且多數缺乏明確目的，此類攻擊技術不高，但數量龐大，對網路安全仍構成持續性的威脅。

6、 內部威脅（Insider Threat）：指企業內部成員利用自身擁有的存取權從事不當行為，其動機可能源於情感、金錢或政治等因素，例如在機場環境中未經授權販售系統存取權，這類行為往往更具隱蔽性與危險性，對企業安全構成重大挑戰。

Example of Cyber Threat Actors Attacks in Aviation

Actors	Attack	Impact
Nation State Actors	Take over Air traffic Management System	Malicious operations camouflage, incidents through misguiding Aircraft in Airspace
Cyber Criminals	Denial of service of Airline Operation Control Center data base	Aircraft grounded => Financial lost
HACKtivists	Airline website defacement	Change the visual appearance of a website to impact Airline reputation.
Terrorists	Corruption of Instrument Landing System	Aircraft collision with ground
Thrill-seeker Hackers	Re-use a known attack scenario to shutdown Flight Information display system	Airport services disruption
Insider Threat	Selling unauthorized access (Airport)	Airport physical attack

圖：航空領域網路威脅者攻擊案例

(三)航空網路安全脆弱點 (Vulnerability)：

航空業因特有的結構和營運模式，塑造了一個複雜的網路環境，普遍具有以下特性：

1、 規模龐大且跨國界：航空業是一個全球性的網路，涉及數千家航空公司、機場、空中導航服務提供者 ANSP (Air Navigation Service Provider)和數量龐大的第三方供應商，這種廣泛互聯的商業模式於企業間網路防護措施薄弱，任一個環節的脆弱點都可能成為全球性攻擊的入口，而跨國界的資訊安全標準也存在監管和技術複雜性。

2、 安全關鍵性 (Safety Critical)：航空公司於遭受網路攻擊後，常造成數據或財務損失，更可能間接或直接影響飛航安全，網路防護措施必須以最高標準實施，因為任何網路入侵或攻擊都可能危及飛航安全或航空管制作業之進行。

3、 環境複雜性：複雜的航空運營環境結合現代化 IT 系統、運行技術(OT)等，可能導致系統中存在多重且難以察覺的脆弱點，系統的複雜性增加了網路安全防護及監控的困難。

(四)航空網路威脅與攻擊途徑 (Current Threat Landscape in Aviation)

1、 首要威脅：如網路犯罪，這類威脅以經濟利益為主要目標，影響航空公司的主要途徑是透過欺詐網站進行詐騙或惡意軟體散播，亦常利用釣魚郵件或惡意軟體滲透航空公司網路，竊取財務數據或進行勒索軟體攻擊等。

2、 上升中的威脅：

(1) DDoS 網路攻擊：分散式阻斷服務 DDoS (Distributed Denial of Service)如針對機場和空中導航服務提供者 (ANSP)的分散式阻斷服務，DDoS 攻擊有明顯的上升趨勢，這些攻擊常與地緣政治緊張/衝突地區有關，目的是透過癱瘓網路中斷關鍵系

統之運作，造成社會和經濟影響，DDoS 攻擊屬於低成本的攻擊手段。

(2) 供應鏈與資料外洩 (Supply Chain and Data Exfiltration)：攻擊者將攻擊目標轉向航空業供應鏈，利用規模較小、安全資源相對不足的供應商作為攻擊跳板，進而滲透到大型航空公司的核心網路造成敏感資料外洩，包括旅客資料、智慧財產權和運營機密等。

3、 飛行安全與地緣政治間影響：雖然迄今尚未有直接影響飛航安全的網路攻擊事件，但於地緣政治緊張(如戰爭)之地區，可能產生間接的連帶影響(例如 GPS 干擾)，這類干擾可能源自於衝突地區的電子戰活動，可能對航機導航系統造成影響。

(五)威脅緩解與保護措施 (Threat Mitigation and Protection Measures)

為了緩解來自各方面的威脅，應建立對抗網路攻擊的防禦體系，有以下的方式：

1、 入侵應對方法：加強網路隔離控制、實施多重要素驗證等。

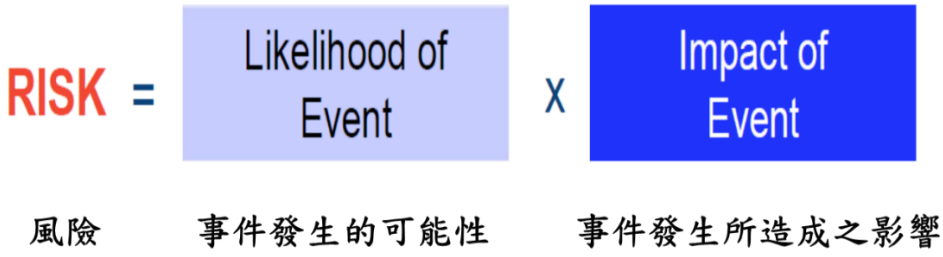
2、 關鍵保護點：加強端點間通訊保護，確保數據於傳輸路徑中從發送端到接收端都保持加密和完整性，防止攻擊或竊取。

3、 人為因素緩解：由於人是安全鏈中最容易被利用的一環，對員工應進行持續的安全意識培訓和建立嚴格的操作程序，以強化安全體系、減少社交工程攻擊發生。

4、 進行風險評估：風險評估是網路安全管理工作的核心，應用威脅 (threat)、弱點 (vulnerability) 和 CIA (機密性、完整性、可用性) 的概念，在資源有限的條件下，排序網路風險優先順序，並規劃緩解措施。

三、 風險管理

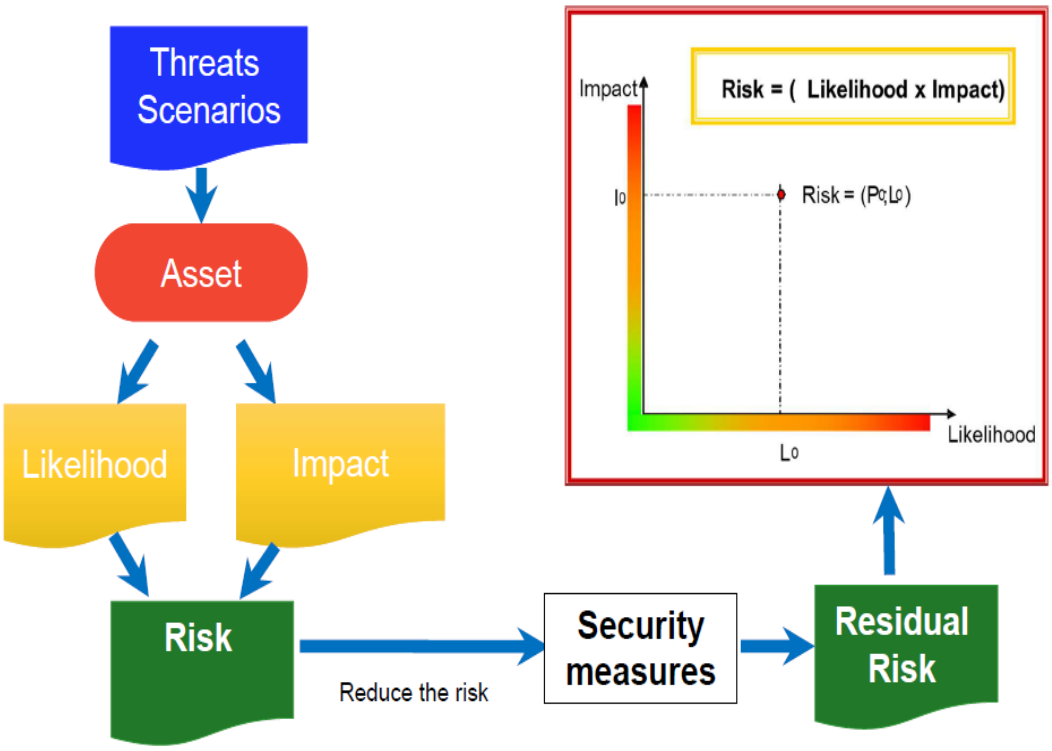
風險，是指在承擔不確定性時，可能導致具有價值的事物（如健康、財富或地位）損失或獲得的潛在性，風險的評估方式多種多樣，有些方法較為複雜，但一種簡單且廣泛使用的評估模型是：



圖：風險評估模型

(一)安全風險管理流程（Security Risk Management Process）

在進行風險評估時，應先確認威脅事件最直接影響的部分(如資產)為何，接著評估該受影響部分損害的可能性與影響程度，據此判定風險等級，並採取相應的緩解措施，以降低風險帶來的衝擊。



圖：安全風險管理流程

(二)事件發生的可能性（Likelihood of Event）

指某件事情發生的機率，風險的可能性，取決於以下三個因素的綜合而成的結果：

1、 自然暴露程度（The Natural Exposure）：即目標資產對於攻擊者的吸引力(例如媒體關注程度)或目標相對於環境的風險狀況。

2、 有罪不罰（The Feeling of Impunity by the Aggressor）：即攻擊被識別的可能性，或攻擊者可能受到的制裁程度。

3、 實現的難易度（The Ease of Realization）：取決於攻擊實現所需專業知能、資源、可透過之途徑及機會等。

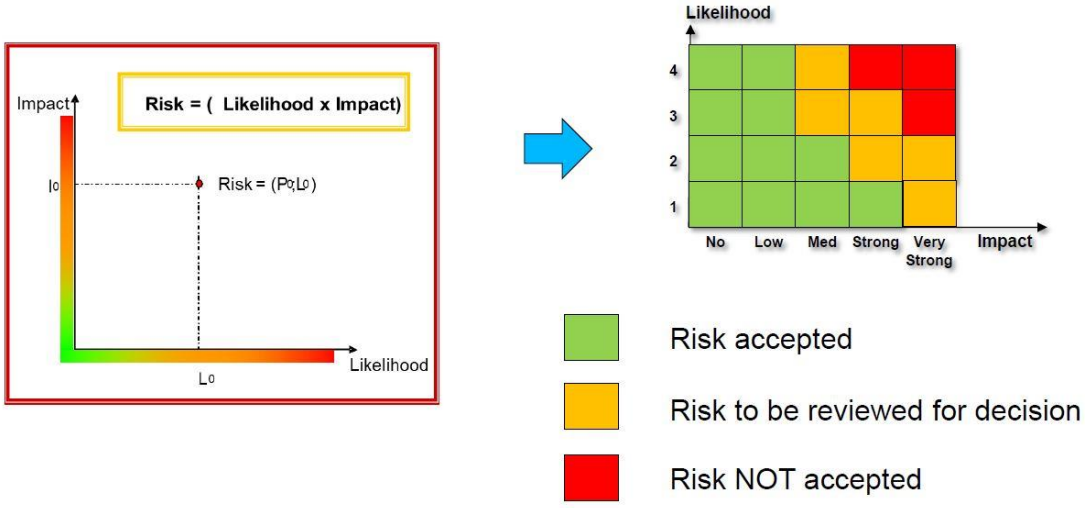
(三)事件發生所造成之影響（Impact of Event）

即攻擊造成的結果，這些結果可能會損害系統的機密性、可用性與完整性，並可能涉及生命安全、實體資產、資料、企業品牌、財務

損失、大眾觀感、隱私權，以及機密資訊外洩等。

(四)風險網格（Risk Grid）

風險網格的運用，是將威脅事件發生的可能性及其所造成的影響量化，並代入風險網格中對應出風險損害程度，並評估該風險損害程度是否已超過可接受之範圍，進而針對威脅事件採行合適之應處，以降低風險損害至可接受的程度。



圖：風險網格

Methods	Countries
EBIOS RM	French
Mehari	French
Octave	United States
Cramm	United Kingdom
SPRINT	United Kingdom
ISO 27002	ISO - International
ISO 13335	ISO - International
ISO 15408 (Common Criteria)	ISO - International
ISO 27005	ISO - International
SCORE	France
CALLIO	Canada
COBRA	United Kingdom
ISAMM	Belgium
RA2	Germany
EUROCAE : Airworthiness security methods and considerations – ED203A	Europe
RTCA : Airworthiness security methods and considerations - DO-356A	United States

圖：國際間採用之風險評估方法（Risk Assessment Methodologies）

(五)進行風險評估（Conducting Risk Assessment）

持續性的風險評估是一項重要的管理流程，它必須以企業內已部設置之程式或關鍵系統為基礎，即時評估網路安全情勢及內部營運條件，並於完成評估後，透過減少安全事件發生的次數（降低可能性）及縮小事件發生後的衝擊範圍（降低影響）之策略，來降低可能發生的損害。

四、 資訊安全事件與事故管理

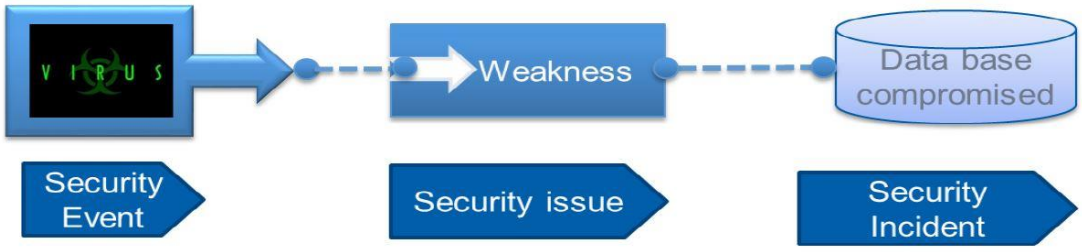
(一)資訊安全事件（Information Security Event）與資訊安全事故（Information Security Incident）

1、 資訊安全事件

指系統、服務或網路的一種狀態、條件或發生情況(且形式多樣，影響程度輕重不等)，該事件發生時即顯示資訊安全可能已遭破壞或入侵，且控制或措施已經失效。

2、 資訊安全事故

由一個或多個不可預期的資訊安全事件所構成，這些事件可能危及企業資訊安全，並削弱或損害企業運作。

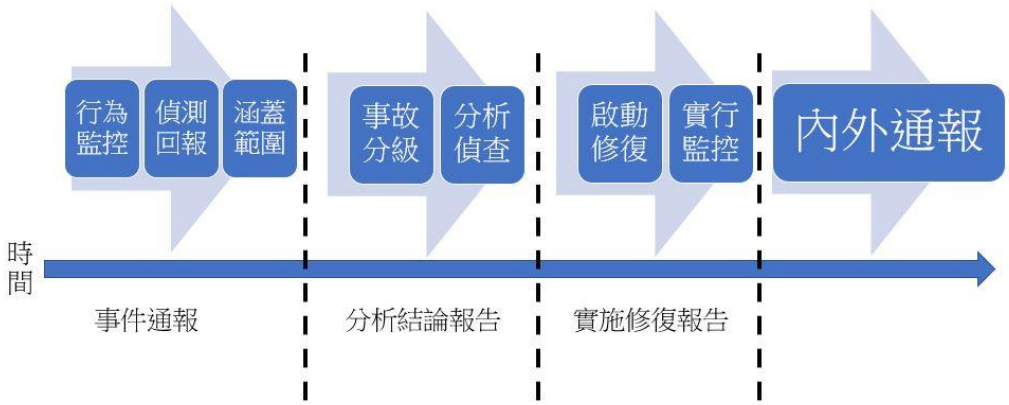


圖：網路安全事故進程

(二)事故管理流程（Incident Management Workflow）

事故管理流程指發生網路攻擊、安全漏洞、系統故障等事件時，企業所採取之系統化應對程序，以最大限度地減少損害、成本和事件

影響的持續時間。



圖：事故管理流程

(三)事故管理職責

1、 資安長（CISO，Chief Information Security Officer）：宣告攻擊正在發生，於執行緩解措施過程中協調事件應變小組，宣告事件已受控制，並統籌分析與監控流程。

2、 電腦緊急應變小組（CERT，Computer Emergency Response Team）：負責確定系統復原的優先順序，以及事件回應生命週期的管理。

3、 安全運作中心（SOC，Security Operation Center）：負責識別、分析與回應網路安全威脅，並在發現安全漏洞時即時通報 CERT。

4、 資訊技術服務台（IT Helpdesk）：作為集中資訊的聯絡窗口，負責接收並回報任何疑似攻擊事件。

(四)事件回應生命週期

事件管理遵循一個標準的生命週期，此週期涵蓋了事件發生前、中、後等 4 個階段如下：

1、 準備階段(Preparation)：進行事故管理，採取系統化應對程序，以最大限度地減少損害、成本和事件影響持續時間。

2、 偵測與分析階段(Detection and Analysis)：

事件發生的初期階段，進行事件的識別及分析，如：

(1) 監控與警報 (Monitoring and Alerting)：透過監控系統識別異常活動或安全警報。

(2) 日誌的重要性 (The Importance of Logs)：日誌是事件發生時的資料來源，可用於追蹤駭客的活動、確定攻擊範圍和方法，必須這些日誌的保護、審查和安全儲存。

(3) 事件分類 (Incident Classification)：根據事件的類型、影響範圍和潛在後果進行排序分類。

3、 控制與復原階段 (Containment and Recovery)：

進行事件處理，以控制攻擊事件並恢復正常運作，如：

(1) 控制(隔離)以防止網路攻擊擴大和蔓延，識別並移除攻擊來源(刪除惡意軟體、修補被利用的漏洞，或禁用被盜用的帳戶等)。

(2) 復原：重從備份檔案中恢復資料、確認系統完整性，並於重新投入運作前進行測試。

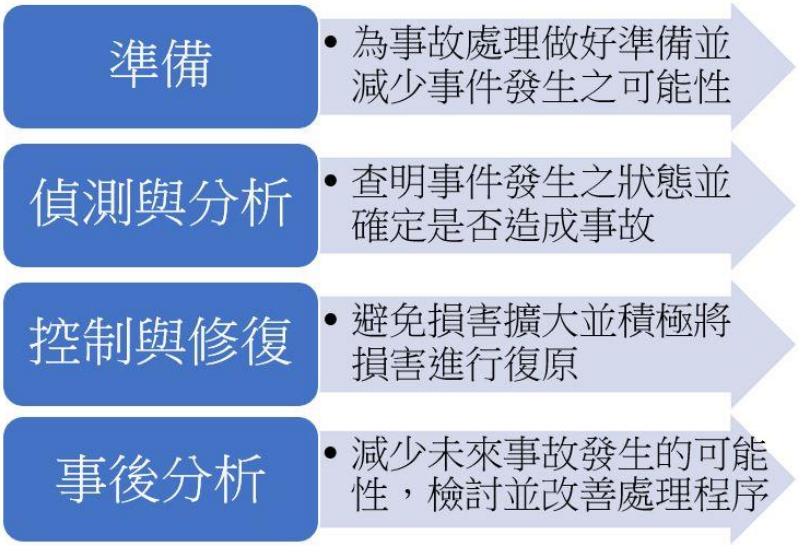
4、 事後分析階段 (Post Incident Analysis)：

於攻擊事件消除後進行分析，並持續進行脆弱點改進，如：

(1) 文件記錄分析：檢視事件發生之紀錄、採取行動、導致事件之原因。

(2) 原因分析：確定事件發生的根本原因。

(3) 流程修訂：依據分析結果，修訂安全策略、流程、技術控制和事件回應計畫，以防止類似事件再次發生。



圖：事件回應生命週期（Incident Response Lifecycle）

五、 航空網路安全法規與標準

網路安全已逐漸成為航空安全之核心議題，且航空網路安全屬非僅依賴航空公司內部相關措施，即可完全排除攻擊之部分，其尚需受國際監管機關訂定之法規及標準予以完善網路安全，就相關規範說明如下：

(一)法規（Regulation）：具有法律 / 規則之效力，其適用為強制性，由具權威的機構（如：ICAO、各國適航主管機關、EASA、FAA、國家安全機構等）訂定。

(二)標準（Standard）：由公認的標準化組織（如：EUROCAE、RTCA）制定並核准，用於產品、相關程序或生產方法等提供準則，一般而言，標準屬於自願性遵循，但若監管機關在法規或認證文件中引用特定標準，則該標準在該情境下即具有約束力。

六、 資訊安全管理系統（ISMS）

資訊安全管理系統 ISMS（Information Security Management System）是一種系統化的方法，用於建立、實施、運作、監控、審

查、維護和持續改進企業資訊安全，其目的在於保護資產的機密性（Confidentiality）、可用性（Availability）與完整性（Integrity），免受威脅影響，並協助防止資訊漏洞被利用。

(一)資訊安全管理系統(ISMS)四大關鍵要素：

1、 高階管理層承諾 (Senior Management Commitment)：制定安全策略與政策、確立責任、設立安全委員會進行決策、設置安全經理、人力資源管理。

2、 持續改進(Continuous Improvement)：進行內部、供應鏈與第三方稽核、安全測試(如漏洞掃描)、持續培訓、變更管理、法規與程序評估修正。

3、 方法/流程/程序與工具管理(Set-up/update)：制定合約與規範、建立網路安全資源庫、確立網路安全標準。

4、 風險與韌性管理(Risk & Resilience Management)：威脅識別、漏洞識別、風險評估與緩解措施執行。

圖：資訊安全管理系統四大關鍵要素

(二)資訊安全管理系統(ISMS)建立

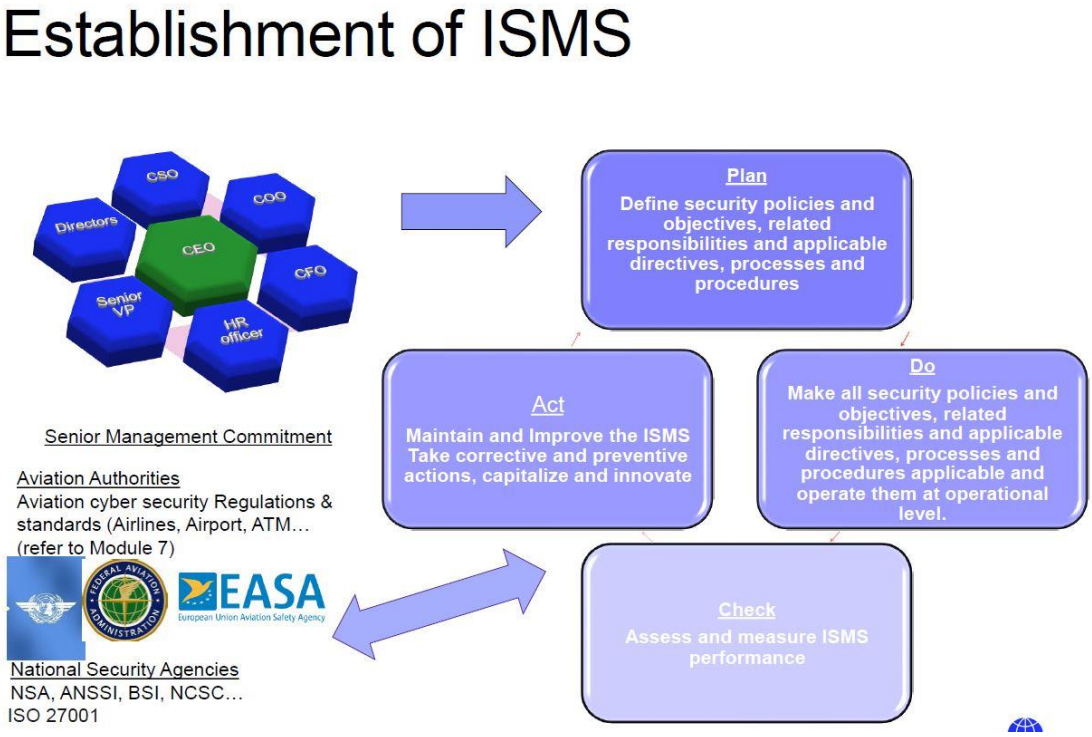
PDCA (Plan-Do-Check-Act)循環模式：

1、 Plan(規劃)：確定安全政策和目標、相關人員職責、流程和程序(如：定義 ISMS 範圍、任命負責人、制定 ISMS 政策、採用風險管理框架)。

2、 Do(執行)：執行安全政策和目標、相關人員職責、流程和程序(如：建立事件與漏洞管理機制、建立內部與外部通報機制、識別與評估風險、處理風險、控制與復原)。

3、 Check(檢查)：評估和量測 ISMS 績效。

4、 Act(行動)：持續評估及改進 ISMS、採取預防措施、經驗累積及創新。



圖：資訊安全管理系統的建立

(三)資訊安全管理系統(ISMS)建立之效益與重要性

1、 效益：

(1) 確保企業符合法規或標準。

(2) 可向主管機關提供佐證資料。

(3) 控制並降低企業風險。

(4) 保護企業聲譽。

(5) 提高顧客對於企業資料安全的信心。

(6) 藉由減少事故發生節省成本。

(7) 提升企業對資安事件的應處。

2、 重要性：

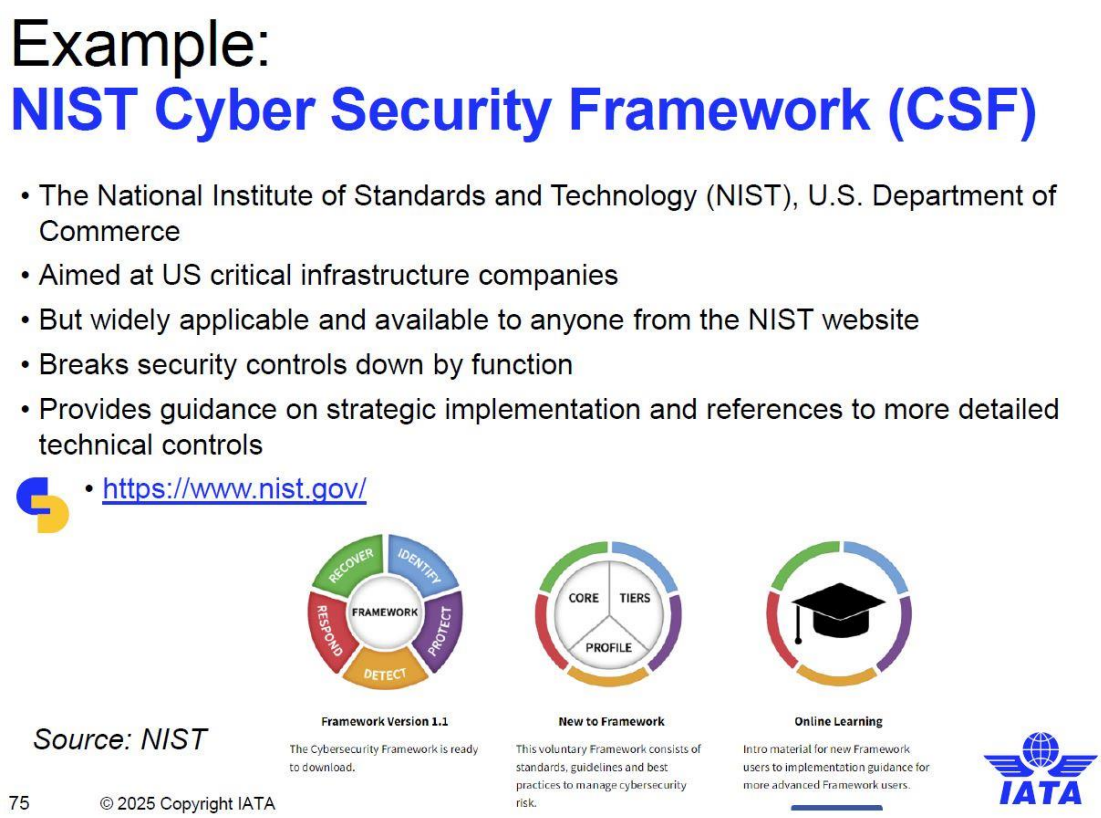
(1) 提供企業安全策略指引。

(2) 可選擇的安全策略眾多，其中以 ISO 27000 資訊安全管理系統與 NIST 網路安全框架（Cyber Security Framework，CSF）為著名。

(3) ISO 27000 資訊安全管理系統標準：由國際標準化組織（ISO）和國際電工委員會（IEC）聯合制定，主要用於建立、實施、維護及持續改進資訊安全管理系統。這套標準在航空網路保安領域，可幫助航空公司、機場、航管（ATC）和飛機製造商確保飛行/旅客資訊/航管系統之安全，減少網路攻擊風險。

(4) NIST 網路安全框架：美國國家標準暨技術研究院（NIST）網路安全框架（CSF）CSF 由五大核心功能組成，這五大功能分別為識別（Identify）、防護（Protect）、偵測（Detect）、回應（Respond）、復原（Recover），形成完整的資訊安全防護應變流程。

圖：ISO 27000 資訊安全管理系統標準



圖：NIST CSF 資訊安全管理系統標準

(四)持續資訊安全維護與改善

資訊安全的維護，並非一次性作業即可完成，由於網路威脅、系統和供應商不斷變化及更新，資訊安全管理系統（ISMS）亦必須配合持續維護和改進，方法如下：

1、 維持資訊安全管理系統(ISMS)運作：

(1) 監控與評估：持續監控威脅、風險、安全事件與事故，並更新相關文件、流程與程序，蒐集回饋以改進不足之處。

(2) 制定關鍵績效指標（KPI），以衡量資訊安全管理系統(ISMS)是否達成預期成效。

2、 稽核：

(1) 企業稽核（Organisational Audit）：主要檢視流程、程序、作法、角色與責任、風險管理及供應鏈管理等。稽核方式包含：針對安全的特別稽核、部門自我稽核、全公司層級的安全稽核或安全審查，以及委託第三方顧問進行外部稽核與審查。

(2) 技術稽核（Technical Audit）：包含滲透測試、漏洞掃描、IT架構檢視等。

(3) 供應鏈稽核（Supply Chain Audit）：提供服務的廠商亦同樣處於不斷變動中，因此對供應鏈進行稽核是有需要的，企業可要求供應商進行自我審查，並隨機抽查其稽核結果，亦可委託第三方單位執行獨立稽核。

3、 品質與保證：

(1) 利用既有的品質控制與保證計畫。

(2) 納入與安全相關的稽核要點與問題。

4、 啟動改善措施：將關鍵問題與改善措施提交高層進行決策，並加以落實執行。

5、 訓練與資訊安全意識提升：

(1) 脆弱點掃描：脆弱點掃描會對指定的 IP 範圍與網域進行檢測，藉由「指紋化」識別(指收集並比對系統特徵，來識別出運行中的作業系統、應用程式或服務)運行中的作業系統與服務，以確保軟體與作業系統即時更新並降低風險的關鍵，且通常包含 e-Discovery(指尋找、蒐集、保存、分析並提供電子形式的資料)的相關步驟。

(2) 滲透測試：由人員主動嘗試繞過安全防線並利用漏洞進行滲透測試，其測試範圍可涵蓋不同層面，從單一應用程式到整個企業皆可進行，亦可藉由以紅隊（Red Team）扮演攻擊者(為測試防護的一方)，藍隊（Blue Team）負責防守(為維護與強化內部防禦一方)，進行滲透攻擊及防禦測試。

(3) 資安意識提升活動：資安意識提升活動可透過多種方式進行，例如內部網路公告、電子郵件電子報、電腦螢幕保護程式中顯示的「每日提醒訊息」。

(4) 持續訓練（Continuous Training）：持續進行防釣魚訓練，以維持員工警覺性。

6、 其他工具使用：如將應用程式(app)開發標準，納入安全性考量。

肆、心得與建議

一、隨著全球航空業隨著數位化的逐漸轉型，先進資訊與通訊技術 ICT（Information and Communication Technology）成為提升效率和飛安的關鍵，但也同時將航空運輸體系暴露於日益複雜的網路威脅之中，網路駭客攻擊目標已從傳統的資訊系統，擴展至更具航空安全的關鍵性的航機通訊、機場營運系統及設施，以及複雜的供應鏈網路。這些威脅包括勒索軟體、分散式阻斷服務攻擊 DDoS (Distributed Denial of Service)，甚至地緣政治影響下的 GNSS (Global Navigation Satellite System)干擾等，對飛航安全構成實質衝擊。

二、作為一名航空保安人員，在過去主要依賴檢查表和資深檢查員經驗傳授累積的知識，惟在面對跨領域、專業化的新型威脅(航空網路保安)，仍需要持續學習及吸收新知才能不斷精進與時俱進。本次「航空網路保安（Aviation Cyber Security)」課程，提供了完整及系統性的課程學習，讓我有機會將網路保安概念重新整合成一個完整的知識體系學習了解，而最核心的收穫，是對於資訊安全管理系統 ISMS（Information Security Management System）系統化管理的認識，並透過 PDCA（Plan-Do-Check-Act）循環，引導企業從政策(策略)制定、防護措施執行，到最終藉由稽核、分析持續改進，形成完整的資安管理流程。然而，ISMS 的建立不僅依賴制度，更有賴於高階管理層的推行與跨部門的合作，以落實 ISMS 的四大要素，同時，課程也強調持續對於網路保安的持續評估改進的重要性，且注重於來自於人為的疏失，因此除了技術防禦外，在提升員工的資安意識及加強教育訓練方面，亦是建立韌性文化的基礎，最後需要應定期檢視及更新資訊安全管理系統，以納入最新的網路攻擊手法、供應鏈威脅等，確保網路保安策略能與時俱進。

三、本次課程之參與學員來自不同國家，讓我有機會與來自瑞士、德國、奈及利亞等國航空專業人士交流及資訊分享，最後引用本次課程講師 Mr. MEHDI AYARI 所言：「跳出框架、像攻擊者一樣地思考，才能在網路保安領域取得成功」，期許自我能持續精進專業職能，運用課程中學習到的系統化 ISMS 框架、風險評估與事件回應等核心知識，於未來的實務工作中，透過更專業、更具前瞻性的視角，協助我國航空站與航空公司進行檢視及強化網路保安之防護。

伍、附錄

結訓證書

Certificate of Completion

This is to certify that

HAOI TAN

born on Sep 26, 1982, has successfully Passed the IATA Classroom course

Aviation Cyber Security

Course duration: Sep 8, 2025 to Sep 10, 2025

Location: Geneva,Switzerland

Course Instructor: MEHDI AYARI

Willie Walsh
Director General, IATA

IATA Training