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：許毓晨 科員

派赴國家/地區：新加坡

出國期間：113 年 12 月 15 日至 19 日

報告日期：114 年 3 月 3 日

提要表

<table>
<tr><td>系統識別號：</td><td>C11400290</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>許毓晨</td><td>交通部民用航空局</td><td></td><td>科員</td><td>薦任(派)</td><td>聯絡人：
yuchenhsu@mail.caa.gov.tw</td></tr>
</table>
</td></tr>
<tr><td>前往地區：</td><td>新加坡</td></tr>
<tr><td>參訪機關：</td><td>無</td></tr>
<tr><td>出國類別：</td><td>其他</td></tr>
<tr><td>出國期間：</td><td>民國 113 年 12 月 15 日 至 民國 113 年 12 月 19 日</td></tr>
<tr><td>報告日期：</td><td>民國 114 年 3 月 3 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>26 頁</td></tr>
<tr><td>報告內容摘要：</td><td>本次訓練課程主要聚焦於航空產業發展數位化所面臨之威脅與挑戰，並探討網路威脅因應對策、風險評估方法及網路安全管理系統（CSMS）之應用，以建立學員對網路安全治理與事故應變機制之概念。藉由參與本次課程，有助於提升對航空網路保安的專業知識，未來可應用於航空保安查核業務，以強化我國航空保安監管效能。</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

本次訓練課程主要聚焦於航空產業發展數位化所面臨之威脅與挑戰，並探討網路威脅因應對策、風險評估方法及網路安全管理系統（CSMS）之應用，以建立學員對網路安全治理與事故應變機制之概念。爰本報告依據課程重要議題分項進行簡述，內容包含網路保安之核心—CIA 三要素（機密性、完整性、可用性）、網路威脅者類型、風險評估模型、安全風險管理流程與風險評估方法、事故管理職責及網路安全管理系統（CSMS）之建立。

藉由參與本次課程，有助於提升對航空網路保安的專業知識，未來可應用於航空保安查核業務，以強化我國航空保安監管效能。

目次

壹、目的

因應科技日新月異，也基於對提升安全性、效率及效益之考量，航空業持續不斷地發展數位化，同時積極引進最新技術，促進產業再升級。數位科技雖有助於航空產業發展，但也隨之衍生眾多且複雜的威脅與風險。國際民航公約第 17 號附約已於 2018 年發布之修訂版中，將航空網路保安之規範增訂其中，旨在要求相關單位進行關鍵資訊及通訊系統之辨識，並採行適當之保護措施，以防範非法干擾行為。觀察近年航空網路安全事件可發現，駭客攻擊標的已從傳統 IT 系統延伸到機上 Wi-Fi、飛機通訊、供應鏈及乘客數據等，攻擊技術亦更趨成熟。因此，網路保安的因應對策亦須與時俱進，才得以確保飛航與資料之安全。

我國航空保安檢查員於執行保安查核、檢查及測試作業時，須確認各航空站及航空公司是否落實航空網路保安相關措施，惟並非所有檢查員皆具備資訊相關知識或專業背景，爰期藉由參與航空網路保安相關課程，了解航空業可能面臨之網路威脅樣態與應處之方式，以及如何透過風險評估與事件管理，建立完善之網路安全管理系統（CSMS），以提升檢查員業務執行之職能，進而對強化我國航空網路保安有所助益。

貳、課程概要

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

二、課程日期：113 年 12 月 16 日至 18 日

三、上課地點：國際航空運輸協會新加坡訓練中心

（IATA Training Center — Singapore）

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，尚有來自香港、馬來西亞、寮國、贊比亞及澳洲之學員參與。

Day 1

Session 1 09:00-12:00
Welcome to the course, meet your fellow attendees and introduction to cyber security
Cyber Threats, Vulnerabilities and Attack Vectors
Lunch Break 60'
Session 2 13:00-17:00
Cyber Threat Mitigation
Exercise 1 - Attack on Supply Chain, Group presentation
Exercise - Airline/Aircraft Risk Assessment, Group Presentation preparation
End of Day 1

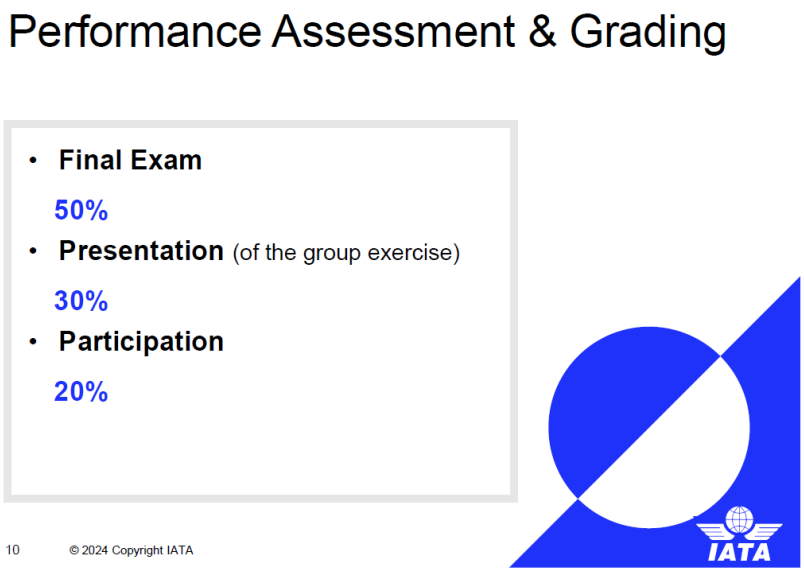
Day 2

Session 1 09:00-12:00
Day 1 review
Risk & Threat Assessment
Exercise - Airline/Aircraft Risk Assessment, Group Presentation preparation
Lunch Break 60'
Session 2 13:00-17:00
Incident Management
Exercise 2 – Airline Operation Center cyber incident
Aviation Regulation
Group Presentation Preparation
End of Day 2

Day 3

Session 1 09:00-12:00
Day 2 review
Setting up a Cyber Security Management System (CSMS) Part 1
Setting up a Cyber Security Management System (CSMS) Part 2
Establishing and maintaining a CSMS
Course Review and exam revision
Lunch Break 60'
Session 2 13:00-16:00
Final exam
Groups assignments presentations
Closure: Group Expectations review

圖：本次訓練之課程大綱



圖：課程評分標準

圖：國際航空運輸協會新加坡訓練中心

參、課程內容

本次訓練課程，主要包含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網路安全管理系統（CSMS）之建立。茲將本次課程內容重點，摘述如下：

一、 課程訓練目標

本次訓練課程目標如下，相關細節內容將分述於後續章節：

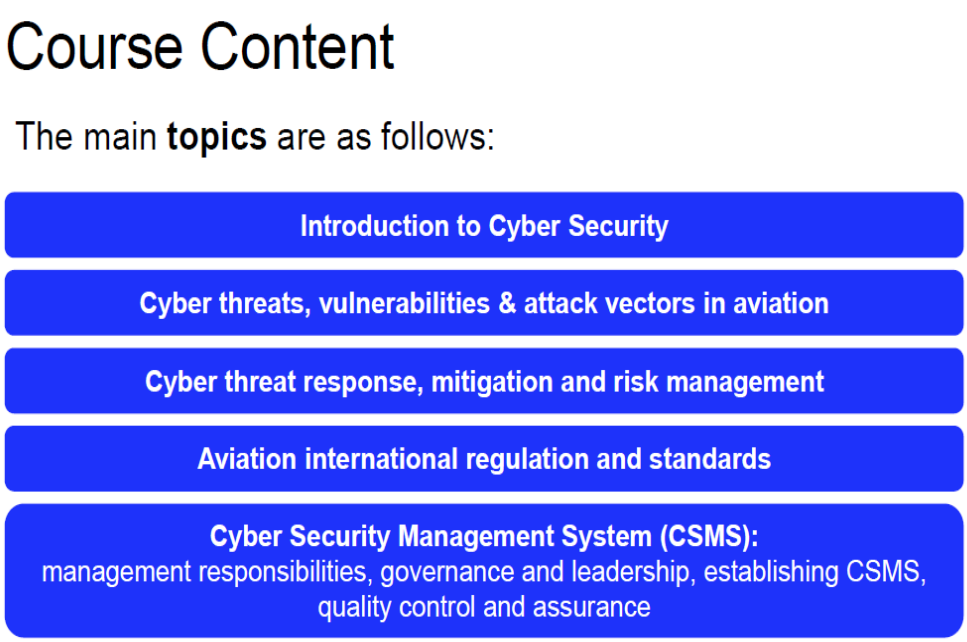
(一)辨識航空網路風險並確定優先級

(二)落實網路風險評估

(三)分析組織網路風險狀況

(四)了解風險緩解流程

(五)建立網路安全管理系統（CSMS）



圖：課程主要議題

二、 網路保安簡介

網路保安可視為對資料（如：客戶紀錄、財務細節、智慧財產權、營運數據等）及系統（如：電腦、行動裝置、應用程式、物聯網、端點等）之保護。雖其定義並未統一，但綜觀國際標準化組織（International Organization for Standardization，ISO）、美國國家標準暨技術研究院（National Institute of Standards and Technology，NIST）、國際電信聯盟（International Telegraph Union，ITU）等各大國際重要機構對於網路保安之闡述，可歸納出以下三大要點，簡稱 CIA 資安三要素（CIA Triad）：

- 機密性（Confidentiality）：確保資訊只有授權人員能取得。
- 完整性（Integrity）：確保資訊不被非法修改。
- 可用性（Availability）：確保資訊能在需要時取得。

圖：CIA 資安三要素

欲維持有效的網路保安就必須在 CIA 三要素中取得平衡，而航空網路保安亦同，且更加重視整體人力與技術之凝聚，以保護航空組織之營運及乘客免於遭受數位攻擊。

(一)網路威脅（Cyber Threat）

1、 定義：任何可能透過系統進行未經授權的存取、破壞、揭露、資

訊修改或拒絕服務等，以致對國家、個人或組織之營運、資產等...產生不利影響的情況或事件。

2、 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，主要目的為竊取政治、經濟、技術或軍事情報等敏感信息，通常具備高複雜度之技術。

(2) 網路犯罪分子（Cyber Criminals）：動機多半是為了獲取利益，行為樣態多元，例如竊取資訊進行轉售等。

(3) 激進駭客（Hacktivists）：藉由破壞目標伺服器或竊取機密資料，進而激起社會性或政治性的效果。

(4) 恐怖分子（Terrorists）：透過破壞行為以取得控制權或攻擊他國。

(5) 尋求刺激駭客（Thrill-Seeker Hackers）：為了獲得樂趣或進行實驗以取得更多關於系統如何運作的知識而採取攻擊，行為複雜程度雖低，但發生案例多。

(6) 內部威脅（Insider Threat）：組織內員工濫用授權進行攻擊，可能是為了報復、獲利或從事間諜行為。

(二)脆弱點（Vulnerability）

1、 定義：可能被一個或多個威脅利用的資產或資產組之漏洞，且其資產是對組織本身、業務運營有價值的任何事物。

2、 產生途徑：配置錯誤（Configuration Errors）、安全控制差距（Gaps in Security Controls）、人為失誤、社交工程（Social Engineering）。

3、 遭受利用方式：例如遠端入侵、破壞系統控制、阻止合法使用者存取系統等。

4、 航空業脆弱特性：環境複雜、供應商眾多、高度科技依賴性且對於攻擊者而言是相當具有吸引力的目標。

5、 機場脆弱點：

(1) 旅客通用處理系統（Common Use Passenger Processing System，CUPPS）：此類設施具有無人值守的特性（例如自助報到機），且通常係利用內部網路連線來存取公司伺服器上的內容，故攻擊者可能輕易地進行的資料存取或篡改。

(2) 行李監控系統（Baggage Scanning Systems）：攻擊者可能利用不安全的 Wi-Fi 連線存取（例如破解 WEP），對系統進行攻擊，擾亂行李運送監管流程或破壞安檢設備之效能。

(3) 通行管制（Pass Control）：攻擊者可能藉由身分冒充或篡改身分驗證系統，進入管制區內進行攻擊或冒充旅客登機。

三、 網路威脅之因應

綜觀國際間歷來發生之網路威脅案例，如資料外洩（Data Breached）、勒索軟體（Ransomware）、阻斷服務攻擊（DoS）、分散式阻斷服務攻擊（DDoS）等，無論是複雜性高或低的網路攻擊事件，威脅者多半都是採用眾所周知的技術，並針對已知的漏洞進行攻擊，這凸顯了做好網路保安基礎防護措施的重要性；為確保有效防範並緩解威脅帶來的損害，可針對以下項目進行檢視及強化：

(一)安全開發演練（Secure Development Practices）：確保開發人員根據關鍵的十大應用程式安全風險（OWASP Top 10） 進行驗證，使其設計之系統得到更完整的保護。

(二)測試（Testing）：定期針對系統之安全性與可用性進行測試。

(三)服務隔離（Segregation of Services）：確保面向外部的服務與內部網路隔離。

(四)防毒軟體（Antivirus）：即時監控並偵測病毒及木馬程式阻擋攻擊。

(五)代理伺服器（Web Proxy）：防止員工誤存取惡意網站或下載惡意執行檔。

(六)加密（Encryption）：減緩資料庫及伺服器遭受非授權人員之入侵。

(七)多重要素驗證（Multi Factor Authentication）：提升認證機制之堅固性。

(八)員工訓練（User Training）：強化員工的網路安全意識，於點擊連結或下載檔案時提高警覺，以避免掉入威脅陷阱。

(九)修補（Patching）：建立脆弱點管理機制，以利及時修復系統漏洞。

(十)管理控制（Administrative Controls）：減少人為因素造成之漏洞。

(十一)資產管理（Asset Management）：控管所有的程式安裝及安裝位置。

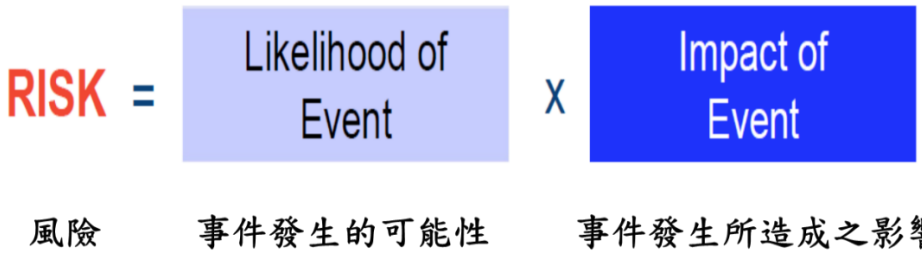
(十二)安全性監控（Security Monitoring）：透過持續掌握資訊安全性、漏洞與威脅之情況，以強化組織風險管理的決策。

(十三)安全事故應變（Incident Response）：為網路威脅事件運用各種方法做好應處。

四、 風險評估與事件管理

風險，泛指損失發生的可能性，而在航空網路保安議題中所談論的風險，應將焦點放在組織中最有價值的資產及與其最密切相關之威脅。

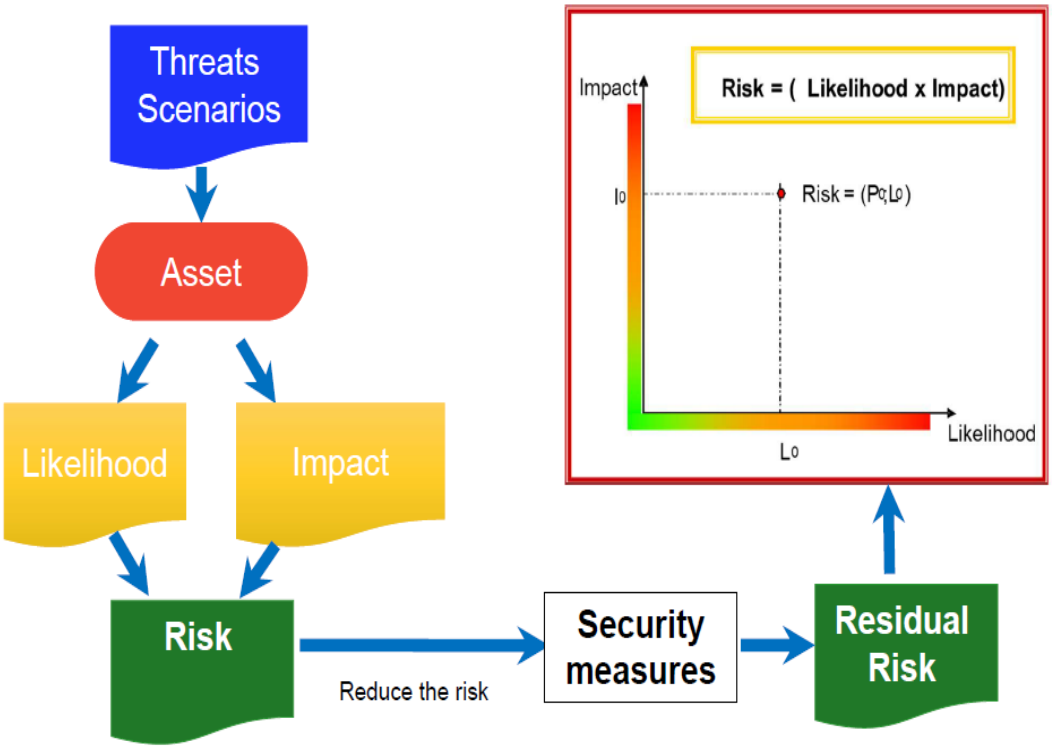
廣泛應用在風險評估之模型如下：



圖：風險評估模型

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

首先應判斷威脅發生後，最直接受影響的資產項目為何，並且針對該資產項目所受到損害之可能性及影響程度進行評估，以得到風險評估層級，進而針對該風險實施相對應之安全措施，以降低最終風險造成的衝擊。



圖：安全風險管理流程

1、事件發生的可能性（Likelihood of Event），可視為以下三大因素集結而成的結果：

(1) 自然暴露（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。

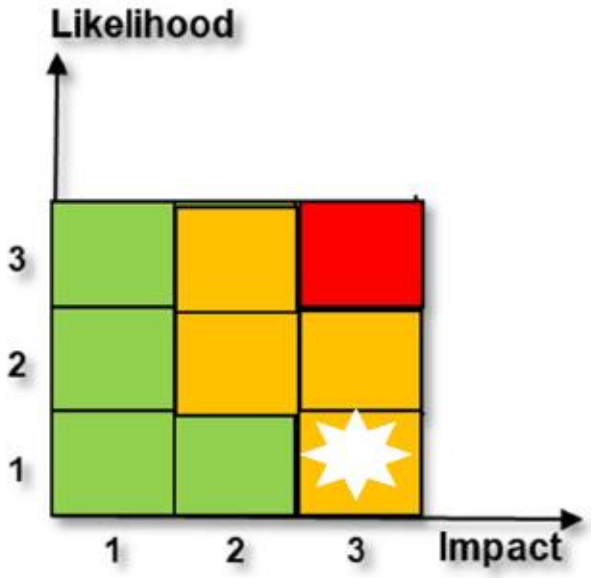
(2) 有罪不罰（The Feeling of Impunity by the Aggressor）：即攻擊被識別的可能性，或攻擊者可能受到的制裁程度。

(3) 實現的難易度（The Ease of Realization）：取決於攻擊實現

所需專業知能、可透過之途徑及可利用之機會。

2、事件發生所造成之影響（Impact of Event），即攻擊行為對CIA三要素產生之損害程度。

3、風險網格（Risk Grid）：將威脅事件發生的可能性及其所造成之影響量化並代入風險網格，可對應出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

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

適用地區	評估方法
ISO國際通用標準	ISO 27002
	ISO 13335
	ISO 15408 （Common Criteria）
	ISO 27005

美國	OCTAVE （Operationally Critical Threat, Asset, and Vulnerability Evaluation）
	航空無線電技術委員會 RTCA ： Airworthiness security methods and considerations—DO-356A
法國	EBIOS （Expression des Besoins et Identification des Objectifs de Sécurité）
	MEHARI （Method for Harmonized Analysis of RIsk）
	SCORE （Systematic Coronary Risk Evaluation）
英國	CRAMM （CCTA Risk Analysis and Management Method） [註：CCTA 為英國中央計算機通信局]
	SPRINT （Situation of Potential Risk resulting from the INTeraction）
	COBRA （Co-Benefits Risk Assessment）
德國	RA2 （Risk Assessment 2）
比利時	ISAMM

	（Information Security Assessment & Monitoring Method）
歐盟	歐洲民用航空設備組織 EUROCAE ：Airworthiness security methods and considerations—ED-203A

(三)安全事件管理（Security Incident and Event Management，SIEM）

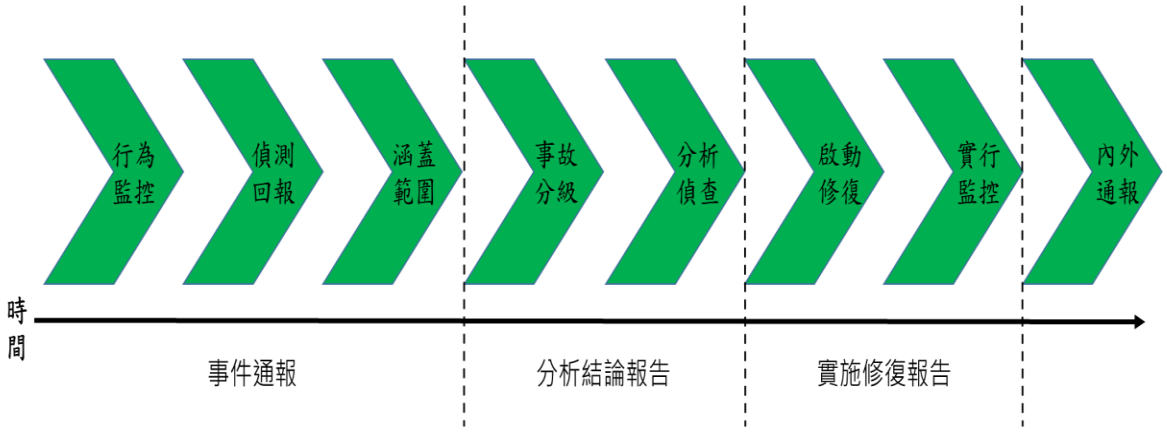
1、 安全事件（Security Event）與安全事故（Security Incident）

(1) 安全事件：係指系統/網路/服務發生違例、失效或不可預期之異常現象。

(2) 安全事故：係指由單一或多個安全事件，實際造成損害之情事。安全事故類型眾多，可能極其嚴重也可能影響微小，例如：電腦/手機/隨身碟遺失、未經授權取得或使用軟體/系統/資料、釣魚信件、內部威脅、阻斷服務攻擊（DoS）攻擊等...。

2、 事故管理流程（Incident Management Workflow）

事故管理流程係指發生網路攻擊、安全漏洞、系統故障等事件時，所採取之系統化應對程序。



圖：事故管理流程

3、 事件回應生命週期（Incident Response Lifecycle）

4、 事故管理職責

(1) 首席資訊保安官（The Chief Information Security Officer）：宣告攻擊的發生，於修復期間監控整體流程進行與協調團隊分工，並於威脅解除後對內/外部通報成果。

(2) 電腦緊急應變小組（Computer Emergency Response Team，CERT）：決定修復優先順序，並依事件回應生命週期（Incident Response Lifecycle）應處。

(3) 安全營運中心（The Security Operation Center，SOC）：識別、分析網路安全威脅並做出反應，並於漏洞發現時通報CERT。

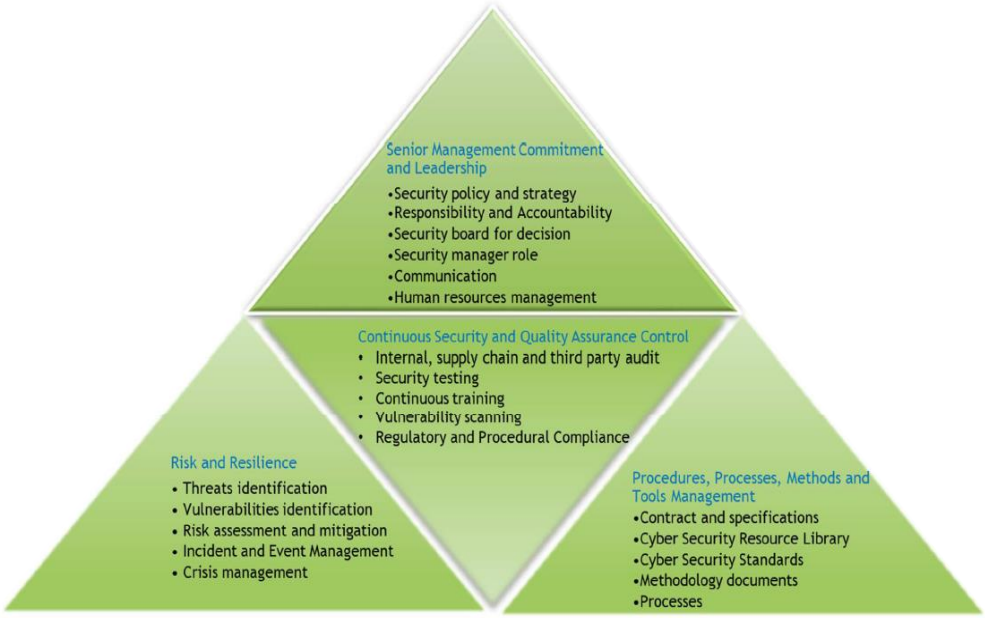
(4) IT 支援服務台（The IT Helpdesk）：作為任何可疑攻擊行為通報之中心聯絡點。

5、 組織日誌收集（Enterprise Log Collection）：組織營運會產生大量的數據紀錄（log data），這些數據的保留及運用對於事件的重建和溯源至關重要。而 SIEM 機制的建立，主要目的便是促使複雜的數

據紀錄能被有效地運用。

五、 網路安全管理系統（CSMS）

建立一套完善的網路安全管理系統（Cyber Security Management System，CSMS）有助於企業進行更有效率的管理，且同時具有以下優點：控制並降低風險、強化事故應處效率、減少因事故衍生之成本、提升企業聲譽及公眾信賴度，同時遵循法律規範。



圖：網路安全管理系統四大主軸

(一)網路安全管理系統（CSMS）四大主軸：

1、 高階管理者承諾（Senior Management Commitment）：

由於航空產業複雜性極高，不僅員工眾多/工作環境各異、擁有龐雜的物流系統及財務資訊，且因跨國須與他國企業和政府交涉，同時又為國家關鍵基礎設施，光靠少數部門以技術維護網路保安是不夠的，必須建立明確的職責分配架構，並由高階管理者領導組織整體共同努力。

(1) 責任分配矩陣（RACI Matrix）：Responsibility 負責者，實際

執行的人；Accountability 當責者，對結果負責的人，通常只有一位；Consulted 諮詢者，能提供意見諮詢的人，可進行雙向溝通；Informed 告知者，布達消息的人。

Example: RACI Table for representing information security roles and assignments

Activities	BOARD	Head of Engineering	Flight Ops	A/C Maintenance	HR	Head of Safety	CISO	...
Risk assessments	A	C	C	C	I	C	R	
Security policies	A	I	I	I	I	I	R	
Incident Management	A	C	C	C	I	C	R	
Secure A/C Data loading	C	R	I	A	N/A	I	C	

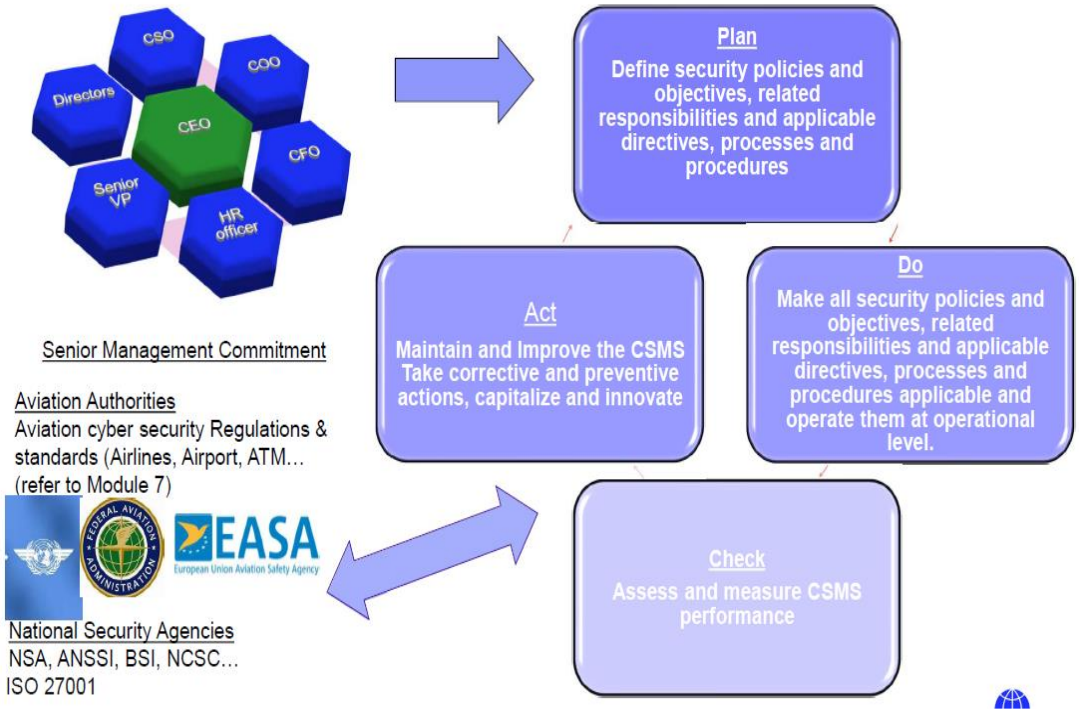
圖：責任分配矩陣範例

(2) 治理與領導（Governance and Leadership）

I. 高階主管領導（Senior Management Leadership）：網路保安牽涉到的不僅僅只是安全本身，更與企業之營運、聲譽、隱私、保密等層面息息相關，故應成為董事會層級的重要議題。透過高階管理層的承諾，更能凸顯網路保安之重要性，並提高企業全體人員對網路保安之重視。

II. 行政階層職責（Executive Level Responsibilities）：執行長（CEO）應確立策略方向並向員工宣告其重要性；首席保安官（The Chief Security Officer，CSO）應負責策略的制定及監督，並協助建構各部門間強而有力的溝通協調

管道；首席資訊保安官（The Chief Information Security Officer，CISO）應負責發展並執行資訊保安計畫，保護企業通訊、系統和資產免受內部及外部威脅；營運長（Chief Operating Officer，COO）應持續掌握網路保安領域的最新動態及最新威脅事件；因各項預算計畫的執行皆涉及網路保安，財務長（Chief Financial Officer，CFO）應完整掌握網路保安政策之運作情形，並能及時反應問題；首席人力資源長（Chief Human Resources Officer，CHRO）應負責員工對於網路保安意識的培訓、維持其個資之保密性，並確保離職員工確實歸還具不可對外洩漏資訊之裝置設備。



圖：行政階層職責

2、 風險評估（Risk Assessment）

3、 事件管理（Management of Incidents）

4、 品質管理（Quality Control and Assurance）：

(1) 品質控制（QC）及品質保證（QA）：由於威脅型態五花八門，系統與應用程式的版本/技術不斷更迭，因此網路安全的管理與維持亦必須與時俱進。透過監控與測量 CSMS 執行的過程，有助於達成有效之品質管理，例如：針對威脅/風險/安全事故(件)進行監控、更新文件資料與程序、根據回饋蒐集進行改善調整，以及透過 KPI 的訂定幫助衡量安全管理之成效是否符合預期目標，並適時啟動矯正措施，將關鍵問題通報高階管理者，俾利其判斷是否調整策略方向與內容。

(2) 資安審查（Security Audits）：包含各部門間與組織整體之稽核，亦可透過第三方諮詢機構進行外部稽查。

(3) 供應鏈管理（Supply Chain Management）：與供應商建立風險共擔的夥伴關係，深入了解供應商的設計體系，且要求供應商應採行自我審查機制，進而建立供應鏈問題資料庫並進行定期查核，以穩定供貨品質。

圖：電子飛行包（Electronic Flight Bag）供應鏈

(4) 意識培訓（Training and Awareness）：定期辦理相關訓練課程，並透過各管道持續傳遞宣導訊息，以多管齊下之方式確保全體員工皆能時刻保持警惕，從最微小的漏洞開始防堵。

(5) 弱點掃描（Vulnerability Scanning）：確保軟體及作業系統穩定保持在有能力抵抗內/外威脅之最佳狀態。

(6) 滲透測試（Penetration Testing）：由組織內部自行模擬網路攻擊情境，一方進行攻擊、另一方負責防禦，從模擬攻防間嘗試揪出可能的安全漏洞，以評估系統的安全性是否足夠。

藉由網路安全管理系統（CSMS）四大主軸，有助於建立一套從理解、預防、偵測、因應到復原的完整控管流程。

圖：網路安全管理系統控管流程

(二)建立網路安全管理系統（CSMS）之流程

1、 確認監管和程序之合規性（Regulatory & Procedural Compliance）：遵守政府或監管機構之規範至關重要，企業應制定出能確實符合要求之系統，且具備足夠靈活度以預測未來的變化。

2、 建立網路安全資源庫（Cyber Security Resource Library）：確保內部及外部之關鍵文件資料皆一併受到保存。

3、 建立網路安全標準（Cyber Security Standards）：應以書面方式明確訂定指導方針，並應持有最新版本且容易取得。

4、 落實合約審查（Contract Reviews）：應針對所有可能影響組織營運之技術與軟體之相關合約內容進行審查。並於簽訂飛機購買協議

時，確認航空器之設計已符合最新安全標準。

(三)網路安全政策（Cyber Security Policies）

網路安全政策（Policies）是網路安全策略（Strategy）的基礎，其內容應包含承諾在企業內部利用網路安全管理系統（CSMS），以確保所有系統都能受到保護且免於遭受資料竊取、損壞及惡意侵害；另，政策應提供並確保整體組織皆採用一致的安全方法。

(四)安全方法論（Security Methodology）

安全方法論是一套系統化的策略與流程，主要用於識別、評估、預防和應對安全風險。在航空網路保安領域，安全方法論之應用範圍涵蓋飛機航電系統、空中交通管理（ATM）、機場 IT 基礎設施及供應鏈安全等。

1、 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，各功能都有其對應之活動與控制措施。這五大功能分別為識別（Identify）、防護（Protect）、偵測（Detect）、回應（Respond）、復原（Recover），形成完整的資安防禦與應變流程。

圖：CSF 五大核心功能

2、 ISO/IEC 27000 資訊安全管理系統標準

由國際標準組織（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、航管機構（ATC）和飛機製造商確保飛行/乘客數據/航管系統之安全，並且減少網路攻擊風險。

圖：ISO/IEC 27000 資訊安全管理系統標準

肆、心得與建議

一、隨著科技發展，航空業已高度依賴資訊系統，從機場運營、飛行管理到機艙 Wi-Fi，都可能成為駭客攻擊的目標。同時，駭客攻擊已從傳統的 IT 系統滲透擴展到飛機通訊、供應鏈管理及乘客數據，這些威脅不僅影響航空公司的運作，也關乎飛航安全與旅客隱私。因此，航空業的網路保安對策必須與時俱進，並整合技術、管理與人員訓練，以建立完整的防禦機制。

二、身為一位新手航空保安檢查員，跟隨前輩同仁進行實務訓練時，經常對於網路保安相關之查核/檢查項目及內容有著諸多疑惑，雖能透過檢查表上之問項、受檢單位之回應說明以及長官同仁的經驗傳授，慢慢拼湊學習網路保安的知識，但因本身對於資訊安全領域了解甚少，在嘗試建構自我職能資料庫的過程中，依舊感覺知識較為零碎，難以組合成型。借助本次訓練課程內容涵蓋之資安管理框架、風險評估與事件管理及案例剖析等關鍵議題，讓我有機會能更深入地瞭解航空產業在發展數位化時所面臨之網路安全挑戰，並且對於如何有效應對網路威脅有了更具體的概念，這將有助於提升未來在執行航空保安查核/檢查時之判斷能力及協助航空公司及航空站強化網路保安。

三、「航空網路保安」與「資訊安全」有著密不可分的關係，課程中也提到，相較於部門個別運作，對抗航空網路保安威脅最有效率的方式，是由高階管理者率領各部門專責人員組成一支獨立的團隊進行應處。然而，於進行實務訓練時觀察我國現狀，航空公司於內部分工上原則還是由不同部門各自依業務權責分派進行網路保安之應處，因此容易產生觀點不一致、資訊不流通的問題。考量現實因素，成立網路保安專責團隊或許有其窒礙難行之處，惟網路保安涉及飛航安全之維護可謂至關重要，應如何改善前述現狀衍生之航空保安疑慮，值得深思。

四、本課程亦提及，許多航空業的資安問題並非僅來自技術漏洞，而是人為疏失所造成的，因此，除了技術層面的防禦外，航空業從業人員的資安意識提升亦是關鍵。我國早已將網路保安相關訓練規定明訂於國家民用航空保安訓練計畫中。惟隨著人工智慧（AI）及物聯網（IoT）技術的發展，駭客採用之攻擊手段亦不斷推陳出新，訓練內容若僅停留在社交工程（Social Engineering）、網路釣魚（Phishing）等固有之案例分享，恐已不足以建立完整之資安意識文化。爰此，各單位辦理網路保安相關訓練課程時，應重視教材之更新，並納入新興案例分享，始能跟上科技快速發展的腳步。

五、本次訓練得與各國航空界專業人士交流並建立良好友誼，實乃寶貴的經驗，亦可作為往後資訊交流之橋梁。引用本課程講師所述：「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。」我將把此次學習到的知識應用於未來實務工作中，並期許能為航空網路保安的提升盡一份力，更期我國能持續派員參與相關國際課程，以利國內相關政策修訂及業務之推行。

伍、附錄

結訓證書

Certificate

This is to certify that

Yuchen Hsu

born on 20 November, has passed the IATA classroom course

Aviation Cyber Security

16-18 December 2024

Singapore, Singapore

given by instructor(s) Mehdi Ayari

Willie Walsh
Director General, IATA

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

0002020074 YAS

IATA Training