Doc 10213 — Unrestricted

Global Cyber Risk Considerations

(FIRST EDITION (advance unedited), 2025)

The ICAO *Global Cyber Risk Considerations* (Doc 10213 – Restricted) contains restricted content and is intended for the limited use of government, industry and other aviation stakeholders involved in cybersecurity for risk assessment purposes. This version of Doc 10213 consists of an unrestricted extract and is available for public distribution.

Notice to Users

This document is an unedited version of an ICAO publication and has not yet been approved in final form. As its content may still be supplemented, removed, or otherwise modified during the editing process, ICAO shall not be responsible whatsoever for any costs or liabilities incurred as a result of its use.

Approved by and published under the authority of the Secretary General

First Edition (advance unedited) — 2025

International Civil Aviation Organization

FOREWORD

The last couple of decades has witnessed a rapid evolution in the use of information and new technologies in the civil aviation sector to support automation, interconnectivity and interoperability goals. This trend has been accelerating in recent times, particularly in the operational areas, in order to benefit from the latest technological developments, such as machine learning and big data analysis. This digitalization will accelerate the deployment of new operational concepts on the ground and in the air and integrate new entrants, such as unmanned aircraft systems (UAS), into the air transport system. The ultimate objective of these developments is to support the growth of the civil aviation sector while enhancing its safety, security, efficiency, capacity and sustainability.

However, this trend has led to an expansion of the cyber threat landscape to include operational systems and information, with the potential for adverse impacts on civil aviation safety, security, capacity and/or efficiency. This has compelled the aviation sector to address cyber threats and risks to civil aviation beyond the traditional Information Technology/Operational Technology (IT/OT) security context so that cyber risk management in aviation is integrated into aviation risk management processes across civil aviation disciplines. This is in support of the protection and resilience of the air transport system through effective and robust risk management frameworks.

The *Global Cyber Risk Considerations* document was developed by the International Civil Aviation Organization (ICAO) to assist Member States and stakeholders in integrating cyber risk management into their aviation risk management processes. It also provides a high-level global cyber threat landscape to emphasize the importance of addressing cyber threats and risks to civil aviation, in support of a resilient and protected sector.

The document supports States and stakeholders in meeting their risk assessment obligations as set out in the Annexes of the *Convention on International Civil Aviation* (the Chicago Convention), particularly their obligations under Standard 4.9.1 in Annex 17 – *Aviation Security*. It also supports the implementation of the ICAO Aviation Cybersecurity Strategy[1] and its associated Cybersecurity Action Plan[2].

The information in this document aligns with the general principles of ICAO guidance on aviation safety and aviation security risk assessment and management processes, as outlined in the *Aviation Security Global Risk Context Statement* (Doc 10108 – Restricted), the *Aviation Security Manual* (Doc 8973 – Restricted) and the *Safety Management Manual (SMM)* (Doc 9859).

This document also includes appendices containing examples of applying the cyber risk management methodology in aviation safety and security risk assessments. The appendices also include guidance on cyber threat categorization, designed to help States and stakeholders identify interdependencies and links between different aviation disciplines. This is intended to support the development and maintenance of a robust risk management framework in civil aviation.

We would like to acknowledge the experts of the Cybersecurity Panel and its Working Group on Cyber Threat and Risk for their valuable contributions of time and knowledge in support of the development of this document.

[1] https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx
[2] https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx

CONTENTS

Page

Abbreviations and Acronyms **4**

Chapter 1. Definitions **5**

Chapter 2. Methodology to Integrate Cyber Risk Management into Aviation Risk Management Frameworks **7**

2.1 Objectives 7
2.2 Overview 7
2.3 Methodology Process Map and Cyber Risk Scoring Tables 10

Chapter 3. Global Cyber Threat and Risk Landscape ..... **x**

3.1 Overview x
3.2 Cyber Risk Assessment Results x
3.3 Analysis of Individual Cyber Risks x

APPENDICES

Appendix 1. Example of Application of the Methodology in Aviation Safety Risk Management Framework **17**

Appendix 2. Example of Application of the Methodology in Aviation Security Risk Management Framework **25**

Appendix 3. Example for Developing a Function Map of Cyber Threat Categories ..... **x**

ABBREVIATIONS AND ACRONYMS

ANSP	Air Navigation Service Provider
APT	Advanced Persistent Threat
ATC	Air traffic control
AVSEC	Aviation security
CPDLC	Controller Pilot Data Link Communications
CRC	Cyclic Redundancy Check
DDoS	Distributed Denial of Service
EATM-CERT	European Air Traffic Management Computer Emergency Response Team
EFB	Electronic Flight Bag
FTA	Fault Tree Analysis
GNSS	Global Navigation Satellite System
HVAC	Heating Ventilation Air Conditioning
IP	Internet Protocol
IT/OT	Information Technology/Operational Technology
IPR	Intellectual Property Rights
MET	Meteorological
NEASCOG	NATO-EUROCONTROL ATM Security Coordinating Group
PBIED	Person-borne improvised explosive device
PII	Personally Identifiable Information
UAS	Unmanned aircraft system(s)

Chapter 1

DEFINITIONS

Access control. Measures to ensure that only authorized access is given to physical and cyber assets.

Attack vector. The means of access which an attacker used to begin an attack.

Availability. Property of being accessible and usable upon demand by an authorized individual, user, programme, process, system or device.

Aviation cybersecurity. The body of technologies, controls and measures, processes, procedures and practices designed to ensure confidentiality, integrity, availability, and overall protection and resilience of cyber assets from attack, damage, destruction, disruption, unauthorized access, and/or exploitation.

Confidentiality. Property that an asset is not being made available or disclosed to unauthorized individual, user, programme, process, system or device.

Critical aviation infrastructure. Assets that are so vital that their incapacity, compromise, or destruction would have a debilitating impact on aviation safety, aviation security, efficiency, and/or capacity.

Cyber asset. Digital and physical items which have value in terms of business, operations, aviation safety, aviation security, efficiency and/or capacity, such as systems, information, data, networks, devices, software, hardware, processes, firmware, relevant/certified personnel, and other electronic resources.

Cyber-attack. The intentional use of electronic means to interrupt, alter, destroy, or gain unauthorized access to cyber assets.

Cyber event. Any observable occurrence in a network or system.

Cyber incident. A single or a series of cyber event(s) that adversely impacts aviation safety, aviation security, efficiency, and/or capacity.

Cyber mitigation. Security control(s) that aim at lowering the cyber risk associated with a specific cyber threat or vulnerability, taking into account their impact on aviation safety, aviation security, efficiency, and/or capacity.

Cyber resilience. The ability of a cyber asset to maintain critical functions under adverse conditions or stress and to recover from those adverse conditions.

Cyber risk. Potential for an unwanted outcome resulting from a cyber event.

Cyber risk assessment. Continuous process of cyber risk identification, analysis, and evaluation.

Cyber risk management. The continuous process of identifying, mitigating, treating and monitoring cyber threats and risks, according to a risk assessment.

Cyber risk matrix. Tool for ranking and displaying components of risks (likelihood, threat, impact/consequence, and vulnerability), risk mitigations, and, ultimately, the residual risks.

Cyber threat. Any potential cyber event that might adversely impact aviation safety, aviation security, efficiency, and/or capacity.

Disruption. A cyber event, whether anticipated or unanticipated, that causes an unplanned, negative deviation from normal operations.

Integrity. Property of accuracy and completeness of an asset, supporting what the asset claims to be.

Reliability. Property that an asset will perform, at the expected level, a required function under specified conditions, without failure, for a specified period of time.

Severity. Qualitative indication of the magnitude of the adverse effect of a threat condition.

Threat entity (or actor). Entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact – an organization or system.

Chapter 2

METHODOLOGY TO INTEGRATE CYBER RISK MANAGEMENT INTO AVIATION RISK MANAGEMENT FRAMEWORKS

Note 1.— In this chapter, aviation functions refer to functions within the different aviation discipline(s) where cyber risk management is integrated into their risk management processes, i.e. aviation safety, aviation security, air navigation efficiency and/or air navigation capacity. In the same context, critical aviation functions are functions that are deemed critical to the concerned aviation discipline(s).

Note 2.— In this chapter, aviation risk management professionals are aviation safety, aviation security, air navigation efficiency and/or capacity risk management professionals, and aviation risk management processes refer to the risk management processes of the concerned aviation discipline(s).

2.1 OBJECTIVES

2.1.1 This chapter supports States and stakeholders in their risk management processes, from risk identification to risk treatment and review, by recommending a generic methodology to integrate cyber risk assessment and management into existing aviation safety, security, and air navigation efficiency and capacity risk management frameworks.

Note 1.— Although the methodology addresses the integration of cyber risk management into aviation safety, security, air navigation efficiency, and capacity assessments, it can be customized to be applicable to any other civil aviation discipline (e.g. business risk management).

Note 2.— Before applying the methodology in this chapter, States and stakeholders may wish to consider areas where existing risk assessment methodologies are commonly recognized by competent authorities as acceptable means of compliance to their specific aviation regulatory requirements, e.g. risk assessments related to aircraft certification.

2.1.2 This chapter addresses aviation safety, security, air navigation and cyber risk management professionals who should work collaboratively to integrate cyber risk management into their respective aviation risk management frameworks across civil aviation disciplines.

2.2 Overview

2.2.1 The methodology presented in this document follows the general concepts of effective risk management cycle described in Figure 1.

Figure 1. Risk Management Cycle

2.2.2 The methodology builds on existing ICAO risk assessment guidance material, namely the ICAO *Safety Management Manual (SMM)* (Doc 9859) and the ICAO *Aviation Security Global Risk Context Statement* (Doc 10108 – Restricted). It takes into account the work of different ICAO expert groups, as well as input from the NATO-EUROCONTROL ATM Security Coordinating Group (NEASCOG), and is also aligned with international standards on cyber risk management (ISO/IEC 27001:2022[3], ISO 31000:2018[4], EUROCAE/RTCA ED201A/DO-391[5], and NIST SP 800-30Rev.1[6]).

2.2.3 Applying the methodology to existing aviation risk assessments of critical aviation functions will provide the following output:

- an updated aviation safety risk assessment that includes the relevant cyber risk assessment;
- an updated aviation security risk assessment that includes the relevant cyber risk assessment;
- an updated air navigation efficiency risk assessment that includes the relevant cyber risk assessment; and/or
- an updated air navigation capacity risk assessment that includes the relevant cyber risk assessment.

2.2.4 Before applying the methodology, it is essential that aviation professionals identify the critical aviation functions in the discipline being assessed. This can be achieved through consultations, surveys, etc., taking into account regulatory and legal requirements applicable to aviation as well as national critical infrastructure.

Note.— The identification of critical aviation functions and their supporting data, information and systems, in combination with the application of the methodology, supports States in their efforts to meet their obligations under Standard 4.9.1 in Annex 17 – Aviation Security to the Chicago Convention[7].

2.2.5 The methodology, depicted in Figure 2 below, should include the following steps.

- **Step 1** – *This step is to be done by relevant aviation risk professionals in collaboration with cyber professionals*.
  - ⇨ Start with an existing aviation risk assessment of a critical aviation function.
  - ⇨ The aviation risk assessment will provide:
    - Minimal Safety Acceptable Level, called Safety Targeted Level;
    - Aviation Security Residual Risk;
    - Minimal Capacity Targeted Level; and/or
    - Minimal Efficiency Targeted Level.
  - ⇨ Identify data, information and systems which support the critical aviation function and tampering of which could impact civil aviation safety, security, efficiency and/or capacity.

Note.— In the event that a critical aviation function is identified for which there is no existing aviation risk assessment, the relevant aviation risk assessment should be conducted and used in Step 1. In the meantime, Step 2 below can be conducted to assess the risk of data, information and systems supporting that function.

[3] https://www.iso.org/standard/27001
[4] https://www.iso.org/standard/65694.html
[5] https://www.eurocae.net/news/posts/2021/december/ed-201a-aeronautical-information-system-security-aiss-framework-guidance/ or https://www.rtca.org/security/
[6] https://csrc.nist.gov/pubs/sp/800/30/r1/final
[7] Annexes to the Chicago Convention, including Annex 17 and its Standard 4.9.1, are applicable to States and not to individual aviation disciplines unless it is specified. Standard 4.9.1 invokes "operators or entities as defined in the National Civil Aviation Security Programme or other relevant national documentation", this language makes the provision applicable to all aviation disciplines as defined at national level by each State.

- **Step 2** – *This step is to be done by cyber professionals in collaboration with relevant aviation risk professionals*.
  - ⇨ Identify cyber threat scenarios that might impact the above data, information and systems, and conduct a cyber risk assessment of those scenarios.
    - Describe the threat scenario including the means and methods of the cyber-attack and the type of threat actor.
    - The likelihood should be evaluated first without taking into account current mitigations. This assesses the threat actor's intent and capability to carry out a threat scenario. This step might include describing, as possible, the threat actor's profile, tools, etc.

Note.— The identified cyber threats should be continuously monitored, to take into account changes in intents and/or capabilities of threat actors.

- The impact/consequence/effect[8] is evaluated in terms of the nature and scale of the specific attack, in relation to aviation safety, security, air navigation capacity and/or air navigation efficiency, under a reasonable worst-case scenario, or worst credible scenario.
- The system's remaining vulnerabilities assessment considers the implementation of existing mitigation measures.
- The output of the above assessment is the Residual Cyber Risk. It is the overall risk remaining after existing mitigations have been considered and the threat likelihood and consequences have been taken into account.

Note 1.— The likelihood, impact and remaining vulnerability ranking tables are described in the following section.

Note 2.— Each organization should define its own cybersecurity objectives and cyber risk acceptance criteria based on applicable aviation and non-aviation (e.g. national cybersecurity authority) regulatory and legal frameworks, as well as its own risk tolerance levels.

- **Step 3** – *This step is to be done by aviation risk professionals*.
  - ⇨ Update Aviation Risk Assessment identified in Step 1. This step will output:
    - Updated Safety Level;
    - Updated Aviation Security Residual Risk;
    - Updated Capacity Level; and/or
    - Updated Efficiency Level.

- **Step 4** – *This step is to be done jointly by aviation risk professionals and cyber professionals.*
  - ⇨ Evaluate the updated Aviation Risk Assessment outputs against the original risk levels obtained in Step 1.
  - ⇨ Risk acceptance criteria should be predefined by the organization and should be comprehensive, covering at a minimum the relevant aviation disciplines (aviation safety, security, capacity and/or efficiency), and cybersecurity objectives and targets.

Note.— Each organization should define its own risk acceptance criteria based on applicable aviation (and sometimes non-aviation) regulatory and legal frameworks, as well as its own risk tolerance levels.

- ⇨ Upon evaluation of the updated outputs versus the original outputs obtained in Step 1, the updated risk of the aviation risk assessment should be deemed unacceptable if:
  - the updated aviation risk assessment does not meet the accepted targets (original risk levels) obtained in Step 1; or
  - the Residual Cyber Risk does not meet the organizational cybersecurity objectives.
- ⇨ If the updated risk is not acceptable, the organization should mitigate the risk by adding specific cybersecurity mitigations where possible and re-evaluate the acceptance of the risk.
- ⇨ If, even after implementing cybersecurity mitigations, the risk is still not acceptable, the organization should define new relevant and effective other mitigations to mitigate the risk to the acceptable levels.

[8] Impact, Effect and Consequence are used interchangeably in this document.

Note.— In case of conflict with regard to risk acceptability between aviation and cyber professionals, the decision should be escalated to the executive organizational level.

- ⇨ In case cybersecurity mitigations are planned, loop back to Step 3.
- ⇨ Ensure that the new cybersecurity mitigation measures do not have a negative impact on the aviation risk assessment. If necessary, take aviation measures[9] or reconsider cybersecurity measures to address any negative impact.

Note.— It is important to consider the potential effect of cybersecurity mitigations on critical data, information and/or systems of other aviation critical functions, as these measures may affect these functions. If such impacts are identified, then a joint assessment of the aviation and cyber risks associated with those critical functions should be conducted.

- ⇨ The assessment should be repeated due to the following reasons:
  - evolution of cyber threats, e.g. existing or new cyber threat scenarios that may become plausible over time, changes in information or knowledge used for the identification, analysis and classification of risks;
  - changes to requirements related to risk assessment in the discipline(s) into which cyber risks are being integrated;
  - functional changes in the evaluated aviation functions; and/or
  - changes in organizational risk appetite and policy on continuous monitoring and assessment and/or risk assessment recurrence.

2.2.6 Appendices 1 and 2 provide two examples of how the methodology can be applied. The first example in **Appendix 1** demonstrates how to integrate a cyber threat into a safety risk assessment. The second example in **Appendix 2** demonstrates how a cyber threat can be integrated into an aviation security risk assessment.

2.2.7 The objective of these examples is to demonstrate that aviation risk assessments and cyber risk assessments cannot be conducted in isolation when considering cyber threats to aviation processes. **It is essential that they interact, coordinate and collaborate with one another in order to provide a comprehensive protection and resilience for civil aviation against cyber threats and risks.**

2.3 Methodology Process Map and Cyber Risk Scoring Tables

[9] Aviation measures refer to aviation safety, security, air navigation efficiency and/or capacity operational measures.

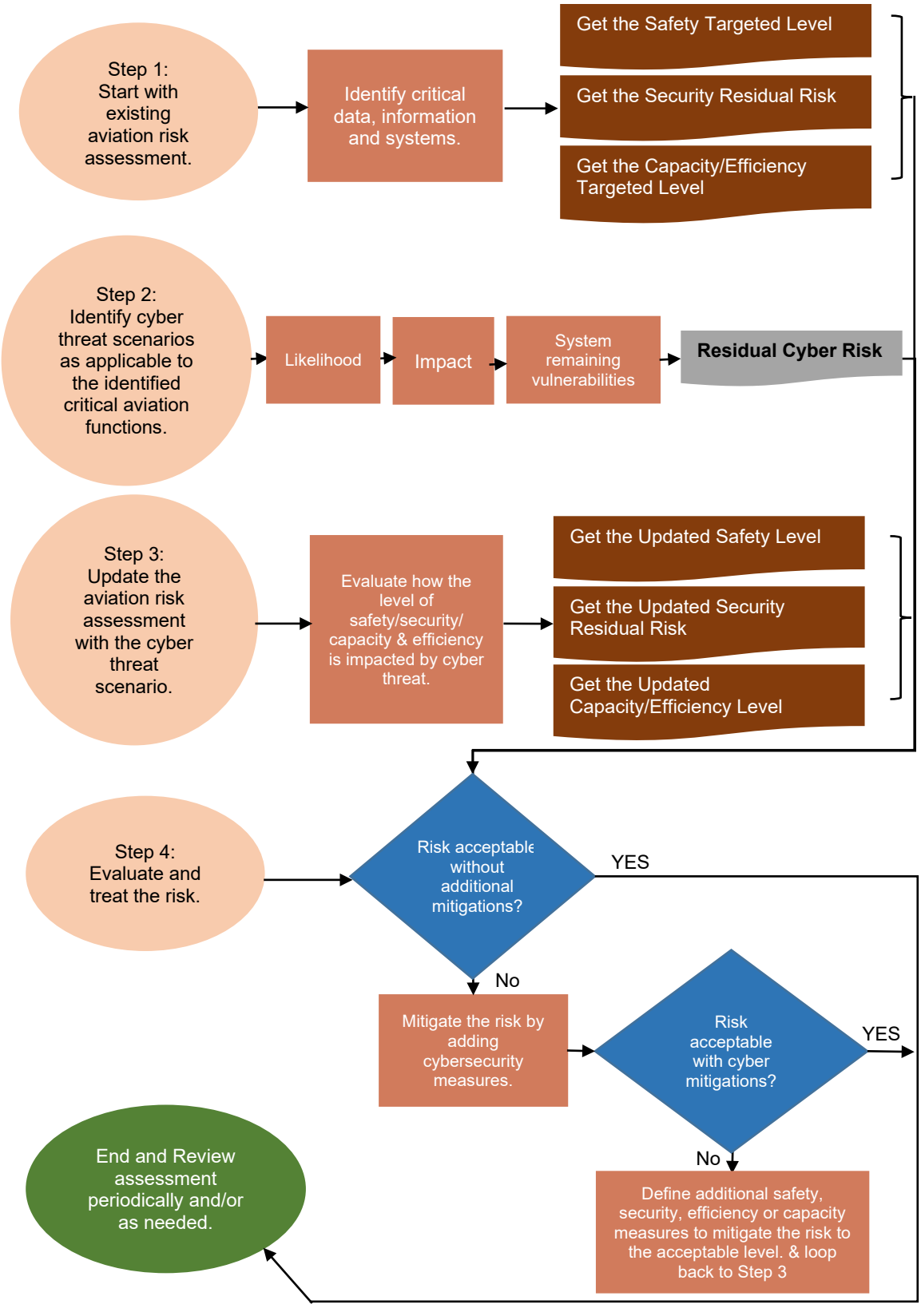


Figure 2. Risk Management Methodology Process Map

Cyber Risk Scoring Tables

2.3.1 The various scoring tables in this section are provided as best practices/guidance on how to build cyber risk assessment matrices. Although they are recommended for the mutual understanding of cyber threats and risks in the context of information sharing[10], these scoring tables can be customized in line with organizations' risk management strategies.

2.3.2 The scores in this section are used to produce the assessments in Chapter 3 of this document.

2.3.3 In this methodology, Likelihood, Impact and Vulnerability are ranked on five levels (HIGH, MEDIUM-HIGH, MEDIUM, MEDIUM-LOW, LOW). Each level is associated with a score and a definition.

Likelihood

2.3.4 The likelihood is the probability of a cyber threat materializing, taking into account the capability and intent of a threat actor to conduct such a cyber-attack.

2.3.5 Likelihood assessment should be conducted by cyber experts, or at the very least by relevant aviation risk experts who have access to cyber threat intelligence reports.

LIKELIHOOD RATING		
HIGH	5	Very plausible scenario, with an actual attack of this kind having occurred in the past few years, or strong evidence of capability and intent.
MEDIUM-HIGH	4	Clearly plausible scenario, with relatively recent examples or evidence of early attack planning or hostile reconnaissance.
MEDIUM	3	An essentially plausible scenario, with some evidence of intent and capability and possibly some examples.
MEDIUM-LOW	2	A scenario for which there are no, or no recent, examples but some evidence of intent, yet with a method apparently not sufficiently developed for a successful attack scenario or probably superseded by other forms of attack.
LOW	1	A theoretically plausible scenario but with no examples, and a theoretical intent but no apparent capability.

Table 1. Cyber Threat Likelihood Ranking

[10] For additional information on cyber information sharing, please see guidance material on Cyber Information Sharing on the following link: https://www.icao.int/aviationcybersecurity/Pages/Guidance-material.aspx

Impact/Consequence/Effect

2.3.6 The impact is the result of measuring in qualitative terms the consequences of a cyber incident on the assets mentioned in the threat scenario description.

2.3.7 The impact assessment should be conducted by aviation experts of the analysed aviation function.

2.3.8 The impacts on aviation safety and aviation security are extracted from ICAO guidance material on aviation safety and aviation security risk assessment respectively in the *Safety Management Manual* (Doc 9859) and the *Aviation Security Global Risk Context Statement* (Doc 10108 – Restricted). The impact on air navigation capacity and efficiency was developed for this document.

IMPACT/CONSEQUENCE/EFFECT RATING[11]			
	Aviation Safety[12]	**Aviation Security**[13]	**Air Navigation Capacity and/or Efficiency**
HIGH **Score = 5**	**Catastrophic:** - Aircraft destroyed	- Hundreds of deaths - Billions of United States dollars - Severe disruption to services and confidence in the aviation system	- Critical disruption to air navigation capacity and/or efficiency. - Widespread outages or complete failure of key operational systems, severely affecting air traffic management or airport operations[14] or airline operations[15]. - Extensive delays or cancellations of flights, posing significant operational risks to the aviation system and the capacity to operate aircraft.
MEDIUM-HIGH **Score = 4**	**Hazardous:** - Serious injury - Major damages - A large reduction of safety margin such that operational personnel cannot be relied upon to perform their tasks accurately or completely.	- Some, but not all, of the impact of the HIGH Consequences	- Significant disruptions to air navigation capacity and/or efficiency. - Extended outages or failures in key operational systems, impacting essential services and capacity to operate aircraft. - Substantial delays in air traffic flow or airport operations or airline operations, resulting in congestion.
MEDIUM **Score = 3**	**Major:** - Injury to persons - Serious incident - A reduction in the ability of operational personnel to cope	- Tens of deaths - Hundreds of millions of United States Dollars - Substantial disruption to	- Noticeable disruptions to air navigation capacity and/or efficiency. - Partial outages or malfunctions in key operational systems, affecting multiple services. - Moderate delays in air traffic flow or moderate impact on airport operations or airline operations, requiring additional

[11] The impact/consequence/effect rating table describes the impact for each aviation discipline where the methodology is used. The columns are independent of each other based on each aviation discipline, and scoring in the first column should be read along with the column specific to the aviation discipline where cyber risk assessment is being integrated.
[12] Aviation safety impact/consequence/effect is extracted from the Fourth edition of the ICAO *Safety Management Manual* (Doc 9859).
[13] Aviation security impact/consequence/effect is extracted from the Third edition of the ICAO *Aviation Security Global Risk Context Statement* (Doc 10108 – Restricted).
[14] Airport operations in this context include all airport services necessary for aircraft arrivals, departures, and taxiing, as well as passenger management, including but not limited to access to gates, availability of security services, runway inspection, baggage handling, fuel, de-icing, catering, airport lighting, and other related services.
[15] Airline operations in this context include all aspects that impact the capacity to operate aircraft in an efficient manner, including: information to flight crews, aircraft maintenance, aircraft operations, MET, availability of GNSS vs non-precision navigation and approach, aeronautical information, etc.

	with adverse operating conditions as a result of an increase in workload or as a result of conditions impairing their efficiency.	services and confidence in the aviation system	coordination and resources to manage.
MEDIUM-LOW **Score = 2**	**Minor:** - Nuisance & operating limitations - Use of emergency procedures - Minor incident	- Some, but not all, of the impact of MEDIUM Consequences	- Minor disruptions to air navigation capacity and/or efficiency. - Limited incident affecting specific systems or services. - Slight delays or inefficiencies in air traffic flow or in airport operations or airlines operations, manageable within normal operational procedures.
LOW **Score = 1**	**Negligible:** - Possibly some injuries - Few consequences	- Possibly some deaths and injuries - Some economic impact - Some disruption to services and confidence in the aviation system	- Minimal disruption to air navigation capacity and/or efficiency. - Isolated incident with very limited impact on overall operations. - Very limited delay or disruptions to air traffic flow, very limited impact on airport operations or airlines operations.

Table 2. Cyber Threat Impact Ranking

Vulnerability

2.3.9 The vulnerability is measured in a qualitative way and describes the effectiveness of existing measures in mitigating the consequences of the cyber threat scenario on the concerned assets.

2.3.10 The vulnerability assessment should be collaboratively conducted between aviation and cyber experts who can analyse the concerned critical aviation function and assess how threat actors may exploit cyber vulnerabilities.

VULNERABILITY RATING		
HIGH	1	No mitigating measures are in effect, either because there are no requirements or because no realistic effective measures are available.
MEDIUM-HIGH	0.8	Mitigation measures have a limited scope, and important areas and aspects of the risk are not covered by requirements or measures in effect.
MEDIUM	0.6	Features of both the MEDIUM-HIGH and MEDIUM-LOW levels are present.
MEDIUM-LOW	0.4	Mitigating measures are generally in place, but they may be immature or only partially effective. For instance, the information security manuals developed by ICAO may be in place for all areas and aspects but in practice, they could be further developed or better implemented.
LOW	0.2	Clear requirements are in place and mitigating measures that are generally regarded as effective are in widespread use.

Table 3. Cyber Threat Vulnerability Ranking

Example of a Cyber Risk Assessment

CYBER RISK ASSESSMENT MATRIX				
Cyber Threat Scenario	**Likelihood** **X**	**Impact** **X**	**Vulnerability**	**= Residual Risk**
A threat actor uses a cyber-attack to impact an aviation asset managed by an aviation stakeholder by exploiting a vulnerability.	**MEDIUM** **3**	**MEDIUM-HIGH** **4**	**MEDIUM-HIGH** **0.8**	**9.6**

CYBER RISK SCORE MATRIX	
RISK SCORE	**RISK RATING**
20-25	HIGH
15-20	MEDIUM-HIGH
10-15	MEDIUM
5-10	MEDIUM-LOW
0-5	LOW

Table 4. Cyber Risk Scoring and Assessment Matrices

APPENDICES

Appendix 1

EXAMPLE OF APPLICATION OF THE METHODOLOGY IN AVIATION SAFETY RISK MANAGEMENT

ASSUMPTIONS AND OVERVIEW

This example illustrates the integration of cyber risk assessment into aviation safety risk assessment, using a hypothetical threat scenario being assessed by an Air Navigation Service Provider (ANSP).

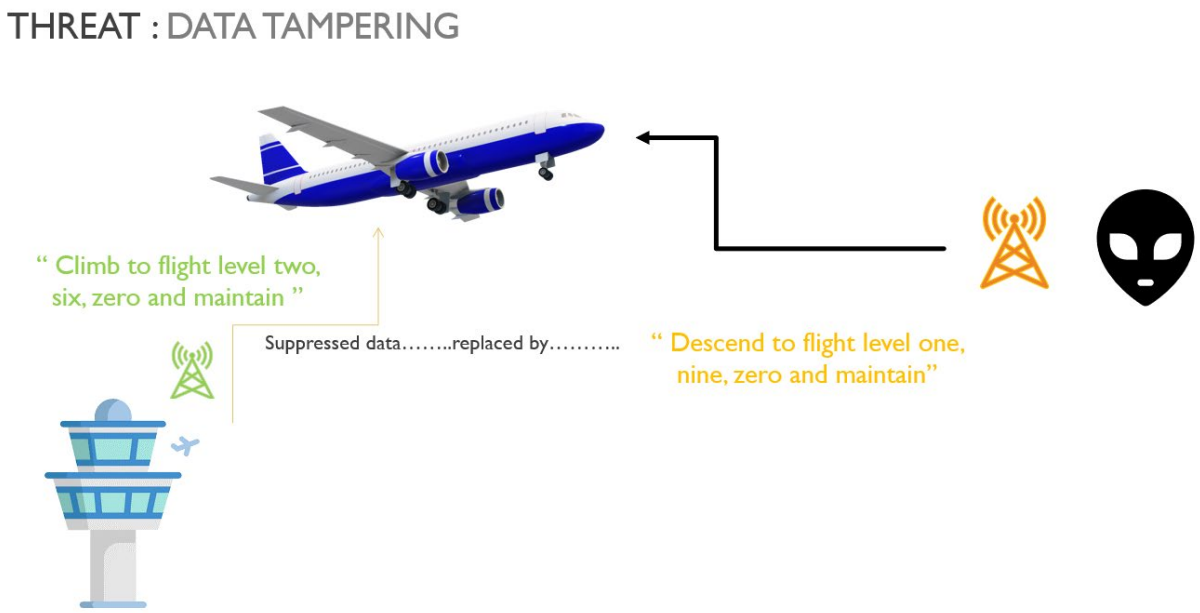
Assumptions:

- ⇨ The ANSP has already assessed, evaluated and mitigated the relevant safety risks using Fault Tree Analysis (FTA)[16].
- ⇨ Aviation Safety experts identified air-ground communication as a critical aviation function.
- ⇨ For simplification purposes, it is assumed that the cyber threat being assessed only impacts safety (no impact on air navigation efficiency and capacity).
- ⇨ The ANSP uses the same scoring tables for likelihood, impact and vulnerability as in this document.
- ⇨ The scoring used for cyber risk assessment uses different values as those in paragraph 3.3.17 above as the scope of the assessment in this example is limited to ground-based systems and data related to CPDLC.
- ⇨ For simplification purposes, it is assumed in the cyber threat scenario below that the impact of the cyber threat is only on CPDLC messages related to flight level clearance.

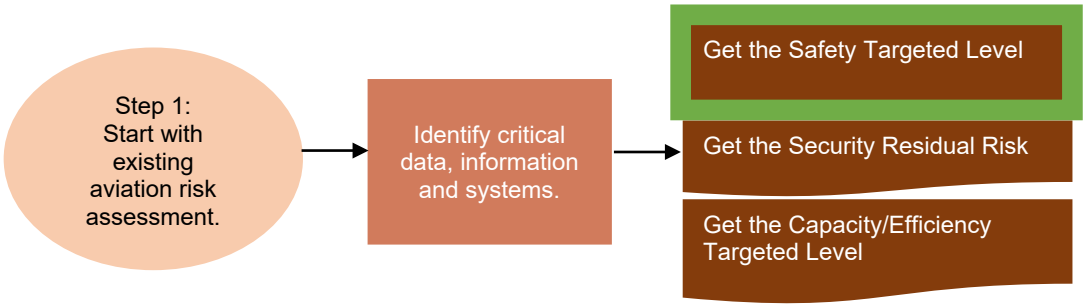
Cyber Threat Scenario:

- ⇨ Aviation Safety experts worked with cyber experts to review existing safety risk assessments for air-ground communications function and identified CPDLC as a system and information supporting the critical function that needed to be assessed for cyber risks.
- ⇨ Aviation Safety experts produced an existing safety risk assessment for a Safety Top-Event covering CPDLC: “Undetected spurious delivery of one or several messages used for providing clearances (Cleared Flight Level – CFL, Direction and Speed) to one or several aircraft”.
- ⇨ Cyber experts, through discussions with aviation safety experts, identified “the data tampering of a CPDLC message sent by an air traffic controller to a pilot” as a cyber threat scenario to be assessed and integrated into the above aviation safety risk assessment.
- ⇨ The scenario being assessed in this example covering an intentional data tampering with a CPDLC message from the controller to the pilot, where an original message (flight level clearance) sent by an air traffic controller to a pilot is tampered with (replaced by an intentionally false flight level) by a malicious actor before its transmission to the aircraft.
- ⇨ For simplification, the attack vector considered is purely on the ground segment of the CPDLC infrastructure: ANSP ground facilities (internal network or servers), or from the communication service provider ground-ground network, or from the air-ground station local network and servers, i.e. the example excludes other attack vectors such as the air-ground communication of CPDLC messages. Using the example for cyber threat categorization in Appendix 3, this cyber threat can be categorized as:
  - ➢ Domain: Air Navigation Service Provider.
  - ➢ Function: Communication, Navigation, Surveillance (CNS).
  - ➢ Sub-Function: Communication.
  - ➢ Cyber Threat: Alteration (modification of message content).

[16] FTA is a tool that supports the identification and analysis of conditions and factors which cause or contribute to the occurrence of a defined undesirable event, usually one which significantly affects system safety, performance, economy, or other required characteristics. FTA is intensively applied to the systems safety assessment.
Guidance on the use of FTA can be found in Part IV of EUROCONTROL’s electronic Safety Assessment Methodology (eSAM) tool: https://www.eurocontrol.int/tool/safety-assessment-methodology, under Part IV Annex K: Fault Tree Analysis Guidance Material.



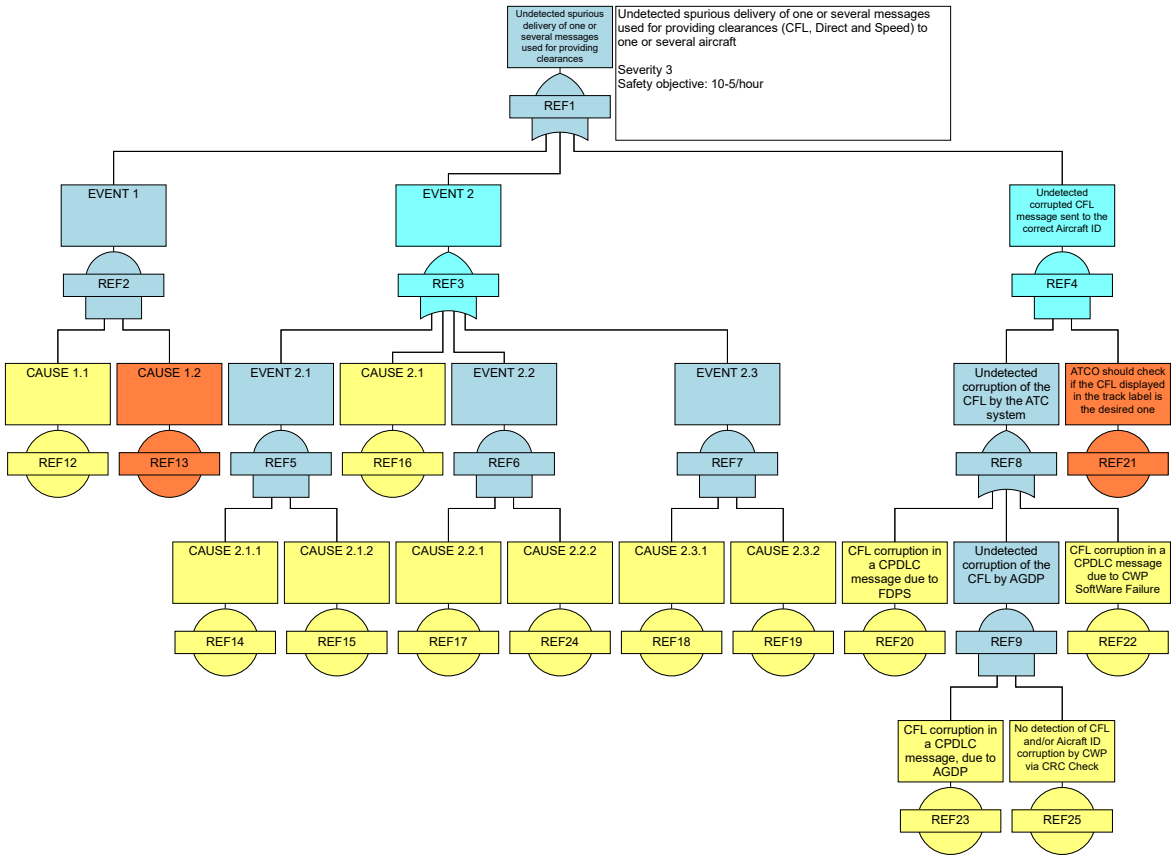
STEP BY STEP APPLICATION OF THE METHODOLOGY



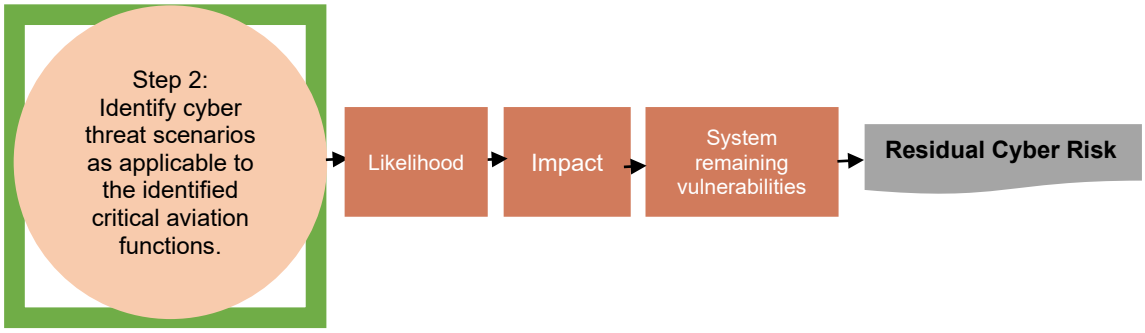
- ⇨ Aviation Safety experts worked with cyber experts to review existing safety risk assessments for air-ground communications function and identified CPDLC as a system and information that supports the critical function that needs to be assessed for cyber risks.
- ⇨ The aviation safety experts produced the original safety Fault Tree diagram[17], without cyber causes. The Top-Level event related to our cyber threat CPDLC scenario is: "an undetected spurious delivery of one or several messages used for providing clearances to one or several aircraft".
- ⇨ **The targeted safety level for the Top-Level event is "no more than 10^-5 occurrence per flight hour".**

[17] Acronyms in the Fault Tree diagram:

- AGDP: Air-Ground Data Link Processor, the Air-Ground Data Server
- CFL: Cleared Flight Level
- CWP: Controller Working Position (the human machine interface)
- FDPS : Flight Data Processing System



Original Fault Tree Diagram

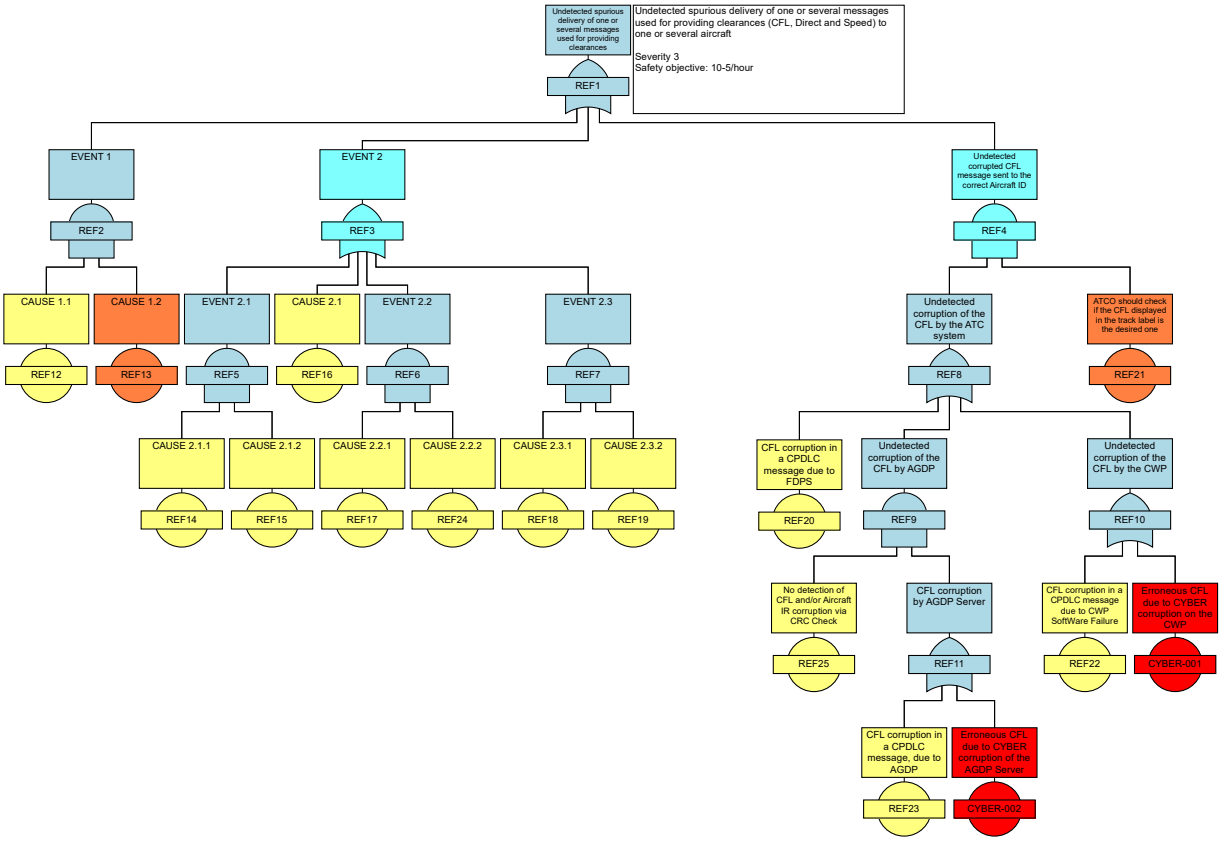


- ⇨ Cyber experts, in collaboration with aviation safety experts, identified “the data tampering of a CPDLC message sent by an air traffic controller to a pilot” as a plausible cyber threat scenario to be assessed and integrated into the above aviation safety risk assessment.
- ⇨ The cyber risk assessment was conducted by the ANSP’s cyber experts in collaboration with safety experts. Cyber experts have knowledge of known methods and attack vectors of cyber threats while safety experts have a knowledge of the architecture of the system.

The cyber risk assessment components in Step 2 are expanded to include the following steps:

The following steps were taken to conduct the cyber risk assessment to build the cyber risk matrix.

- **Likelihood:**
  - Safety experts often use probabilities for likelihood (e.g. number of occurrences per flight hours). Also, when using fault trees, some experts use the "distance" from the Top-event in the fault tree to estimate the likelihood (e.g. the further from the Top-event, the lower the likelihood of it impacting the Top-event in terms of altering the targeted safety level). On the other hand, cyber experts often use likelihood tables with discrete values (such as Table 1 in Chapter 2). The objective of this joint work between experts is to align understanding of the different risk components.
  - As such, in this example, inserting the cyber threat into the fault tree (the red elements) facilitates the estimation of the likelihood in terms of capability and intent of the cyber threat materializing.[18]



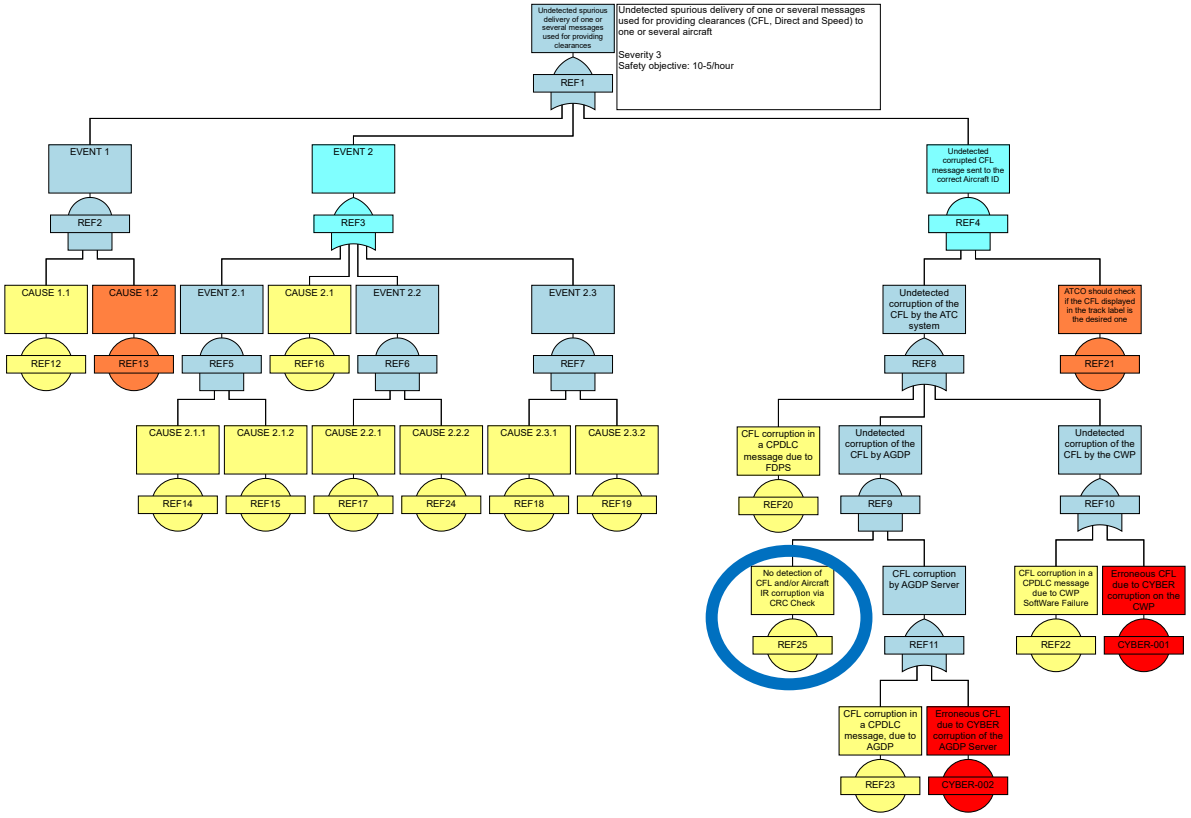
Updated Fault Tree Diagram

  - The likelihood of the cyber threat was established to have a score of 2 which corresponds to MEDIUM-LOW (i.e. a scenario for which there are no, or no recent, examples but some evidence of intent, yet with a method apparently not sufficiently developed for a successful attack scenario or probably superseded by other forms of attack).

- **Impact/Consequence/Effect:**
  - Assessing the impact involves evaluating a reasonable worst-case scenario, which in this case means that the cyber-attack was successful, and the Top-Level event was not prevented. As such, the impact assessment assumes the highest severity possible of the Top-event before the introduction of the cyber threat, which is and corresponds to an impact level of MEDIUM (Major safety impact: "A serious incident with a reduction in the ability of operational personnel to cope with adverse operating conditions as a result of an increase in workload or as a result of conditions impairing their efficiency.").

[18] In a complete cyber risk assessment, many attack vectors may be added to the original diagram. The example includes only two possible attack vectors for simplicity.

- **Vulnerability:**
  - Vulnerability assessment is conducted taking into account existing mitigation measures.
  - In this regard, the FTA indicates that a Cyclic Redundancy Check (CRC)[19] of the CPDLC message is performed. As such, it is taken into consideration as well as measures related to IT Security (protection of systems and servers) and aviation security (background checks and access control).



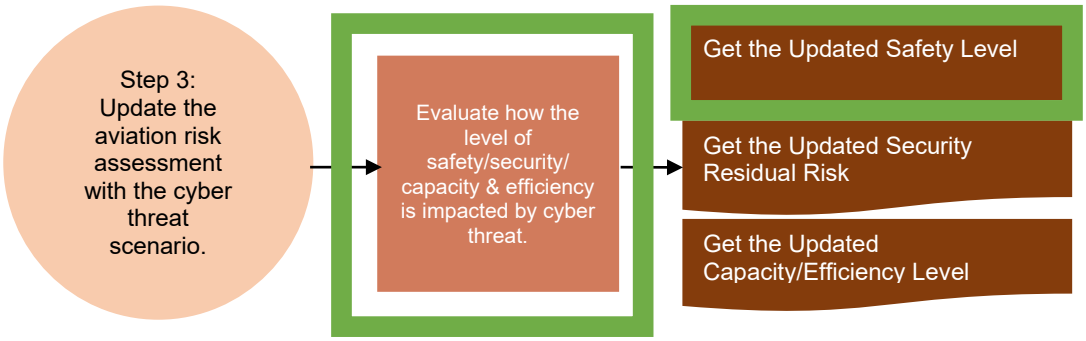
  - Cyber experts are aware that CRC is mainly used to detect unintentional errors in the data. CRC is not effective against intentional interference as the attacker is able to change the CRC hash along with the change in the message and therefore, the cyber experts' conclusion is that existing cyber controls might not be enough to mitigate the risk.
  - Also, the vulnerability assessment led to the conclusion that an external cyber-attack would be somehow difficult to prepare and execute. The ANSP's communication networks and systems are adequately protected against external attack and the organization has implemented adequate monitoring and detection capabilities. Internal attack (insider threat) would be relatively easier to organize as physical security measures implemented are also adequate (access control to relevant rooms and background checks of personnel with access to those areas).
  - Accordingly, the vulnerability is given a score of MEDIUM-HIGH (0.8).

- **Residual Cyber Risk:**
  - The Residual Cyber Risk can now be calculated by multiplying the likelihood, impact and vulnerability scores**: 2 x 3 x 0.8 = 4.8**.
- The Residual Cyber Risk score of 4.8 has been rounded to 5 as it was considered by the experts to be closer to MEDIUM-LOW than LOW.

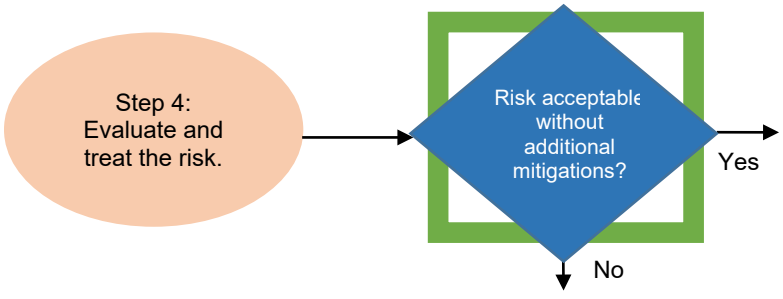
[19] CRC is defined as "A method to ensure data has not been altered after being sent through a communication." – Source: NIST SP800-72

The Cyber Risk Matrix will then be as follows.

CYBER RISK MATRIX					
Scenario	**Likelihood**	**Impact**	**Mitigations**	**Vulnerabilities**	**Residual Risk**
Intruder tampering with the data payload of a CPDLC message sent from a controller to a pilot.	**Score of 2** MEDIUM-LOW A scenario for which there are no, or no recent, examples but some evidence of intent, yet with a method apparently not sufficiently developed for a successful attack scenario or probably superseded by other forms of attack.	**Score of 3** MAJOR Top safety event: Undetected spurious delivery of one or several messages used for providing clearances.	CRC Monitoring and intruder detection capabilities already implemented. IT Security measures Physical access control/background checks	**Score of 0.8** MEDIUM-HIGH CRC is not a suitable tool to detect malicious tampering of information as it can be tampered with along with the information.	**Score of 4.8 (rounded to 5)** MEDIUM-LOW This score will be compared to the other threat scenario scores and used to rank the threats.



- ⇨ Now that the fault tree diagram has been updated, and the organization knows a lot more about the cyber threat translated into a cyber risk corresponding to safety objectives, the original safety risk assessment can be updated including the evaluation of the cyber threat, leading potentially to a new probability of occurrence of the safety Top-Level event ("Undetected spurious delivery of one or several messages used for providing clearances").
- ⇨ This will serve as a basis for the next steps: risk evaluation and risk treatment.

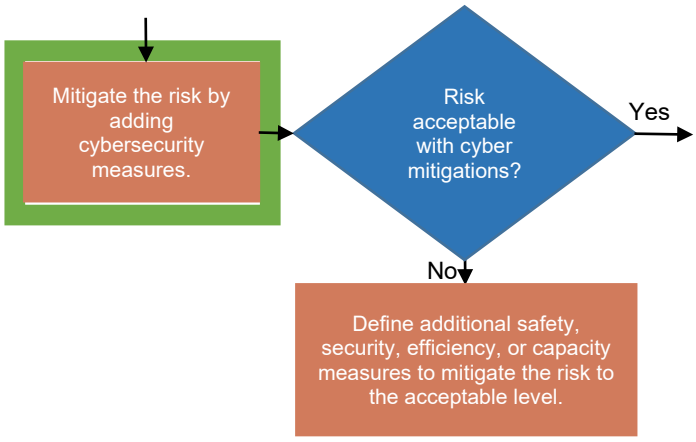


With the updated assessments, the ANSP uses its existing acceptability matrix. This acceptability matrix may contain different types of criteria such as:

- Cyber criteria, the source of which includes aviation regulations, critical infrastructure regulations/laws, organizational risk tolerance, etc.
- Safety criteria, which include the relationship between the safety impact and the safety targeted likelihood as well as sources related to relevant aviation regulations.
- Air navigation capacity and efficiency criteria which is organization dependent (and outside the scope of this example).

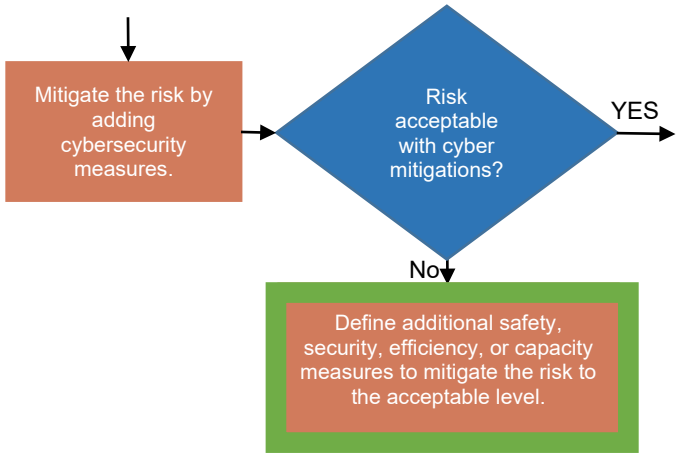
This assessment against these organizational criteria should lead to a decision: **Can the risk be accepted as is or should cyber mitigations be put in place in complement existing controls?**

The evaluation led to the decision that although the Residual Cyber Risk is MEDIUM-LOW, it is decided to consider additional mitigations that could bring down the risk even further.



⇨ **Cybersecurity Mitigations**:

- ➢ Cyber experts proposed first the addition of new equipment to further protect the system from interference. However, this addition was rejected by safety experts as it would create new points of failure that would require the review of the whole safety assessment of the system, as well as other impacted systems.
- ➢ Safety and cyber experts agreed that the controls in place to protect the system against an outside cyber-attack are adequate, and therefore decided to look for measures to mitigate the insider threat which was agreed as more plausible during the cyber risk assessment.
- ➢ Cyber experts proposed measures that tighten access privilege on the relevant computers and servers which was accepted.



⇨ **Additional mitigations**

- With these cybersecurity mitigations, it was determined that the risk can be further reduced by considering other types of mitigations.
- Aviation security experts proposed tighter background checks and access control measures for personnel given access to the ATC and server rooms.
- The evaluation of the risk was repeated taking into account the new mitigations (both cyber and AVSEC measures) and it was decided that the new mitigations would reduce the risk to an acceptable level, so the new measures were accepted for implementation.

⇨ **Cyber Risk Matrix**

- This led to the completion of the cyber risk assessment matrix with additional mitigations to be recorded for implementation, and the final cyber risk assessment matrix became as follows.

CYBER RISK MATRIX						
Scenario	**Likelihood**	**Impact**	**Mitigations**	**Vulnerabilities**	**Residual Risk**	**Supplementary Mitigations**
Intruder tampering with the data payload of a CPDLC message sent from a controller to a pilot.	**Score of 2** MEDIUM-LOW A scenario for which there are no, or no recent, examples but some evidence of intent, yet with a method apparently not sufficiently developed for a successful attack scenario or probably superseded by other forms of attack.	**Score of 3** MAJOR Top safety event: Undetected spurious delivery of one or several messages used for providing clearances.	CRC Monitoring and intruder detection capabilities already implemented. IT Security measures Physical access control/background checks	**Score of 0.8** MEDIUM-HIGH CRC is not a suitable tool to detect malicious tampering of information as it can be tampered with along with the information.	**Score of 4.8 (rounded to 5)** MEDIUM-LOW This score will be compared to the other threat scenario scores and used to rank the threats.	**Cyber: Optimization and monitoring of digital access privilege on relevant computers and servers.** **Other: Tighter background checks and physical access control for personnel given access to the ATC and server rooms.**

CONCLUSION

The step-by-step approach in this example is provided for illustration purposes to show how safety and cyber risk assessments need to interact to address cyber threats and risks to civil aviation. In a real environment, this process would take place in a more iterative and integrated manner, depending on the organizational governance structure and regulatory/legal frameworks in place.

— — — — — — — —

Appendix 2

EXAMPLE OF APPLICATION OF THE METHODOLOGY IN AVIATION SECURITY RISK MANAGEMENT

ASSUMPTIONS AND OVERVIEW

The example given below illustrates the integration of cyber risk assessment into aviation security risk assessment, using a hypothetical threat scenario being assessed by a State.

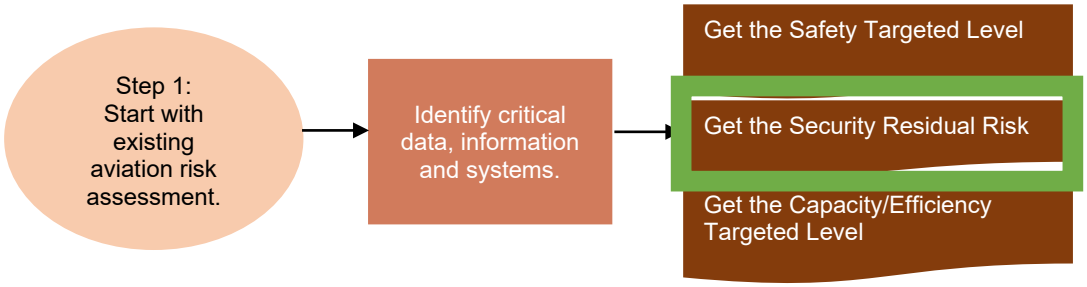
Assumptions:

- The State has already assessed, evaluated and mitigated the relevant aviation security risks using AVSEC Risk matrices.
- Aviation security experts identified cabin baggage screening as a critical aviation function.
- For the purposes of simplification, it is assumed that the cyber threat being assessed only impacts aviation security (no impact on safety, air navigation efficiency and/or capacity).
- The State uses the same scoring tables for likelihood, impact and vulnerability as those used in this document.
- The scoring used in the cyber risk assessment uses the same values as those in Chapter 3 for consistency. However, in reality, the likelihood, impact and vulnerability scores of individual States and organizations' will vary according to the different variables that affect these ratings (capabilities, intent, existing mitigation measures, etc.).
- Due to the sensitivity of aviation security risk assessments, only the process to integrate the cyber risk assessment into the aviation security assessment is described. The cyber risk assessment process is described in detail.

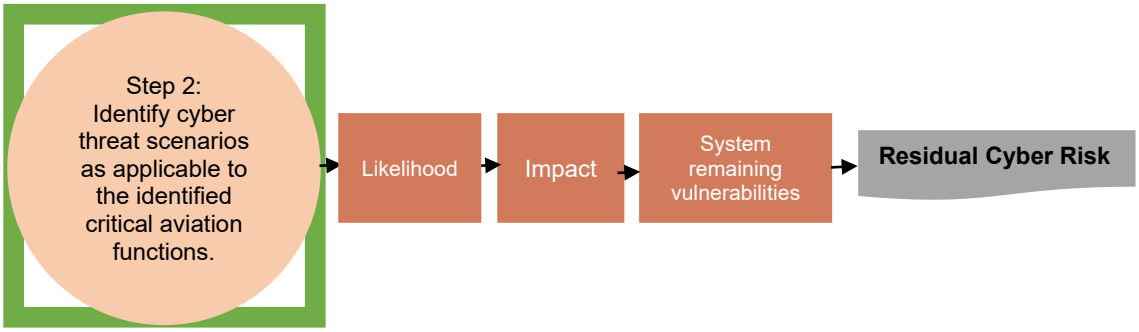
Cyber Threat Scenario:

- The State is analysing the different possible modus operandi of an adversary attempting to bring person-borne improvised explosive devices (PBIEDs) on board an aircraft in cabin baggage with the intention of bringing down the aircraft.
- Aviation security experts worked with cyber experts to review existing AVSEC risk assessments for cabin baggage screening and identified the detection component of the screening equipment as a critical system and information (supporting the critical aviation function) that should be assessed for cyber risks.
- Aviation security experts have produced an existing security risk assessment for PBIEDs (on the body or in cabin baggage) and considered only the latter for this assessment exercise.
- Through discussions with aviation security experts, the cyber experts have identified "the data tampering of the detection component with the aim to alter the outcomes of the automated screening process" as a cyber threat scenario to be assessed and integrated into the above aviation security risk assessment.
- Attack vector: this attack could be carried out through interference with equipment detection capabilities through physical or remote access to the equipment in question.
- Using the example for cyber threat categorization in Appendix 3, this cyber threat can be categorized as:
  - Domain: Airport.
  - Function: Security.
  - Sub-Function: Cabin Baggage Screening.
  - Cyber Threat: Alteration (Interference with detection software/systems).

STEP BY STEP APPLICATION OF THE METHODOLOGY



- ⇨ Aviation security experts worked with cyber experts to review existing security risk assessments for PBIEDs in cabin baggage and identified the detection component of the screening equipment function as a system and information supporting the critical function that needs to be assessed for cyber risks.
- ⇨ The aviation security experts produced the initial risk assessment of PBIEDs without cyber causes. The aviation security scenario related to our cyber threat scenario is: "Prohibited item brought on board by passenger with the intent of bringing down plane".
- ⇨ **The result of this process is to get the Security Residual Risk for the above scenario.**



- ⇨ Cyber experts, in collaboration with aviation security experts, identified "the data tampering of the detection component with the aim to alter the outcomes of the screening process" as a plausible cyber threat scenario to be assessed and integrated into the above aviation security risk assessment.
- ⇨ The cyber risk assessment was conducted by the State's cyber experts in collaboration with aviation security experts. Cyber experts have knowledge of the known methods and attack vectors of cyber-attack while aviation security experts have a knowledge of the equipment and its tolerance levels.

The cyber risk assessment components in Step 2 are expanded to include the following steps:

The following steps were taken to conduct the cyber risk assessment in the field of aviation security to build the cyber risk matrix:

- ⇨ **Likelihood:**
  - ➢ Both aviation security experts and cyber experts often use likelihood tables with discrete values (such as Table 1 in Chapter 2), which helps to align the understanding of the different risk components.
  - ➢ The capability to execute the cyber-attack being assessed would require a thorough preparation.
  - ➢ An external attack is difficult to carry out since the screening equipment is either stand-alone (not connected to a network) or connected to a local closed network, and would require a lot of effort and know-how to alter the outcome of the screening process.

- An insider threat is possible, but it would require a lot of effort and know-how to alter the outcome of the screening process, for example:
  - Detailed knowledge of the airport, screening check points, schedules, etc.
  - High level of cooperation is needed (attack cannot be carried out without help).
  - Access to the machines and/or to the local network is required.
- There is some evidence of intent today.
- As a result, the likelihood of the cyber threat was set at 3, which is MEDIUM (i.e. an essentially plausible scenario, with some evidence of intent and capability and possibly some examples).

⇨ **Impact/Consequence/Effect:**

- Assessing the impact involves evaluating a reasonable worst-case scenario, which in this case means that the cyber-attack was successful.
- The result of the cyber-attack would be a false output of the screening equipment, potentially missing prohibited items. This could lead to the destruction of the aircraft, hundreds of fatalities, possibly some on the ground. Another consequence would be very high immediate costs and long-term economic damage. The impact would therefore be HIGH (score of 5).

⇨ **Vulnerability:**

- The vulnerability assessment is conducted taking into account existing mitigation measures.
- Regarding existing mitigations:
  - The State has mandated ICAO Annex 17 – *Aviation Security* Standards and Recommended Practices for passenger screening using detection systems implemented by the airport.
  - The State also requires its operators to implement Standard 4.9.1 and Recommended Practice 4.9.2 related to addressing cyber threats, and the airport is therefore implementing the following measures:
    - There is a logical[20] or physical separation in IT networks from commercial/operational infrastructure.
    - Background checks are applied to staff and aviation security measures are in place to protect access to equipment.
- Cyber experts have confirmed that the controls already in place are satisfactory to mitigate the cyber risk. However, as aviation security experts are aware that the requirements implemented by the airport are not consistently implemented worldwide (especially those related to Recommended Practices), it was agreed to score the vulnerability as MEDIUM-LOW (0.4).

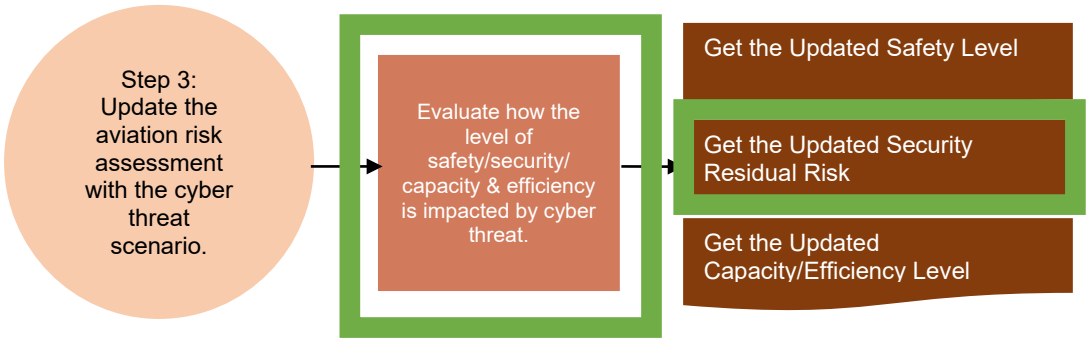
⇨ **Residual Cyber Risk:**

- The Residual Cyber Risk can now be calculated by multiplying the likelihood, impact and vulnerability scores: **3 x 5 x 0.4 = 6, leading to a Residual Cyber Risk of MEDIUM-LOW.**

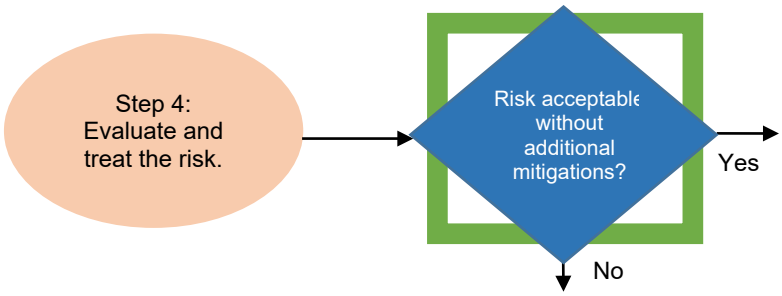
20 Logical separation refers to network segmentation through creation of logical (virtual) zones on the same physical network or hardware.

The Cyber Risk Matrix becomes as follows.

CYBER RISK MATRIX					
Scenario	**Likelihood**	**Impact**	**Mitigations**	**Vulnerabilities**	**Residual Risk**
Prohibited item brought on board by passenger with the intent of bringing down the plane, by alteration of security screening equipment outcomes.	**Score of 3** MEDIUM Is an adversary capable? Is there an interest to attack a civil aviation target?	**Score of 5** HIGH In the reasonable worst-case scenario: how many lives will be lost? Is damage to infrastructure expected? Will the public lose confidence in air transport? What is the economic cost?	ICAO Annex 17 Standard 4.9.1 and Recommended Practice 4.9.2 are applied to screening of passengers using detection systems.	**Score of 0.4** MEDIUM-LOW After considering the current mitigating measures, how vulnerable is aviation to this threat scenario?	**Score of 6** This score will be compared to the other threat scenario scores and used to rank the threats.



- ⇨ Once the cyber threat is translated into a cyber risk corresponding to aviation security objectives, the initial aviation security risk assessment can be updated including the evaluation of the cyber threat, which is now addressed in the Aviation Security Risk Matrix for the scenario in question, potentially leading to a new Security Residual Risk.
- ⇨ This will serve as a basis for the next steps: risk evaluation and treatment.



- ⇨ With the data information, the State will update its PBIED risk matrix to include this modus operandi.

This evaluation should result in a decision: **Can the risk be accepted as such, or should cyber mitigations be implemented in addition to the existing controls?**

- ⇨ It was concluded that the Residual Cyber Risk was too low to change the original assessment, and therefore the residual risk of the overall PBIED-type threat scenario is not affected by this cyber threat scenario (i.e. the aviation security threat remains at the same higher level).
- ⇨ Cyber experts were also satisfied with the controls in place to support the integrity of the screening process.
- ⇨ However, cyber experts noted that any change to the equipment requires recertification of the equipment by the relevant authority, which may expose the system to future cyber threats if discovered vulnerabilities cannot be rectified in a timely manner. As such, a project has been initiated to find a balanced approach between certification and updating cybersecurity controls on screening equipment, and the outcome of the project has been recorded as an additional mitigation measure for future implementation to support cyber risk mitigation.
- ⇨ The updated cyber risk matrix for this scenario is therefore as follows.

CYBER RISK MATRIX						
Scenario	**Likelihood**	**Impact**	**Mitigations**	**Vulnerabilities**	**Residual Risk**	**Supplementary Mitigations**
Prohibited item brought on board by passenger with the intent of bringing down the plane, by alteration of security screening equipment outcomes.	**Score of 3** MEDIUM Is an adversary capable? Is there an interest to attack a civil aviation target?	**Score of 5** HIGH In the reasonable worst-case scenario: how many lives will be lost? Is damage to infrastructure expected? Will the public lose confidence in air transport? What is the economic cost?	ICAO Annex 17 Standard 4.9.1 and Recommended Practice 4.9.2 are applied to screening of passengers using detection systems.	**Score of 0.4** MEDIUM-LOW After considering the current mitigating measures, how vulnerable is aviation to this threat scenario?	**Score of 6** This score will be compared to other threat scenario scores and used to address the threats.	Developing processes to balance patching of vulnerabilities and recertification of cabin baggage screening equipment.

CONCLUSION

The step-by-step approach in this example is provided for illustration purposes to show how aviation security and cyber risk assessments need to interact to allow for addressing cyber threats and risks to civil aviation. In a real environment, this process would take place in a more iterative and integrated manner, depending on the State/organization's governance structure and regulatory/legal frameworks in place.

— END —