International Civil Aviation Organization

Thirteenth Meeting of the Common aeRonautical Virtual Private Network Operations Group (CRV OG/13)
Wellington, New Zealand, 05-08 March 2025

Agenda Item 14: Cyber-safety/security and resilience

REVIEW OF THE CANSO CYBER SECURITY RISK ASSESSMENT GUIDE

(Presented by New Zealand)

SUMMARY

This paper presents the outcomes of the review of the CANSO cyber security risk assessment guide

1. INTRODUCTION

1.1 At the twelfth meeting of the Common aeRonautical Virtual private network operations group (CRV OG/12) Denarau Island, Fiji 23-26 January 2024, it was suggested that the CANSO cyber security risk assessment guide could be a good document for the CRV OG to review and potentially adopt.

1.2 We have captured some risks in the past using the Airways New Zealand Risk Assessment Framework, however this is very specific to Airways operations.

2. DISCUSSION

2.1 The CANSO cyber security risk assessment guide is a document that is freely available from the CANSO website.

2.2 It is part of a collection of documents as shown below.

2.3 Whilst the cyber security risk assessment guide focused on cybersecurity risk, the concepts in this document could be used to provide a risk assessment framework for the CRV.

2.4 The Guide provides guidance risk assessment on the following areas:

1. Risk Assessment scope
   The first step in conducting a risk assessment consists of understanding the general mission of the organisation. The mission is a high-level description of the purpose of the organisation aimed at aligning all stakeholders involved in the risk assessment activity.

2. Risk Assessment
   RISK IDENTIFICATION The purpose of risk identification is to determine what can happen to cause a potential loss (confidentiality, availability and integrity), and to identify how, where, and why the loss can happen.
   - Identification of the primary assets
   - Identification and analysis of impact
   - Identification of the supporting assets
   - Identification and analysis of threat scenarios

   RISK ANALYSIS A risk analysis may be qualitative or quantitative. Often organisations lean to a qualitative approach due to the lack of accurate and reliable data to support a quantitative approach. The output of the risk analysis is a defined risk level for each identified risk which is derived from the defined impact and threat level.

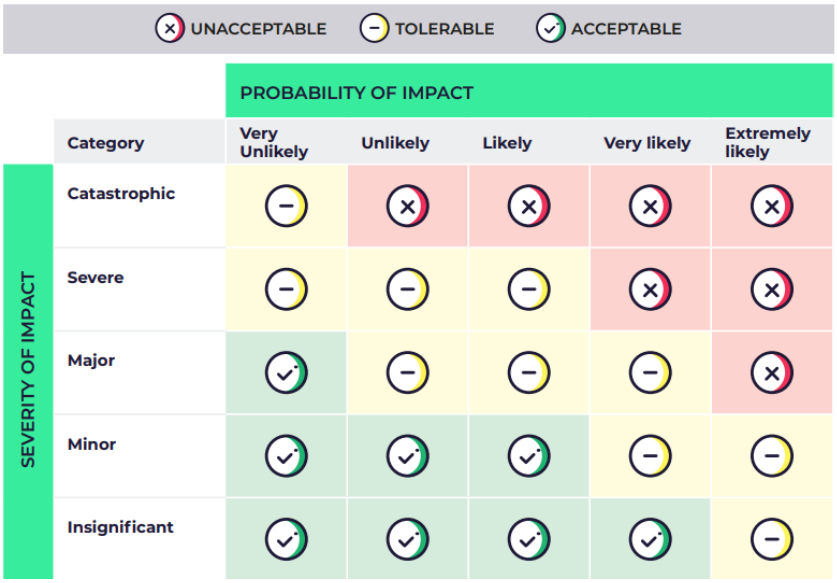
   RISK EVALUATION When the risk level is determined and benchmarked against the risk acceptance criteria, it will provide guidance as to the scope of mitigating efforts that need to be developed to control the risk.

3. Risk Mitigations and Monitoring
   To fully assess the cybersecurity risks on the net-centric aviation system performance, several activities need to be undertaken. These include the performance of a cost benefit analysis relating to the introduction of relevant cybersecurity functions and the determination of suitable policies, procedures, and processes to support a holistic cybersecurity posture. A key aspect is the presence of detection mechanisms which need to be established to identify the presence of a threat, and decision support tools for threat evaluation and mitigation. Once a threat has been detected it is management's responsibility to consider ways in which their organisation can address that threat, including the mitigation and monitoring mechanisms.

4. Risk Acceptance
   Risk acceptance indicates that an organisation is willing to accept the level of risk associated with a given activity or process. There may be times when the risk level resulting from a risk assessment process is not defined as acceptable, but an organisation may choose to accept the risk because all other alternatives are unacceptable

5. Risk Communication and Consultation.
The purpose of risk communication and consultation is to help relevant stakeholders affected by the risk to understand the risk and gain support for the necessary mitigating actions. Communication will promote awareness and understanding of the risk whereas consultation will be in the form of feedback and information to support decision-making.

2.5 The Risk Assessment matrix is focusses on whether the risk is Unacceptable, Tolerable or acceptable.



2.6 Whilst the ICAO Doc 9859 - Safety Management Manual (SMM) covers the same concepts, it is possible to use the CANSO framework to create a CRV Risk assessment and associated process and procedure at an acceptable level for the CRV.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information contained in this paper; and

b) discuss any relevant matter as appropriate

– – – – – – – – – – – – –