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 GUIDE

(Presented by New Zealand)

SUMMARY

This paper presents the outcomes of the review of the CANSO Standard of Excellence in Cyber Security

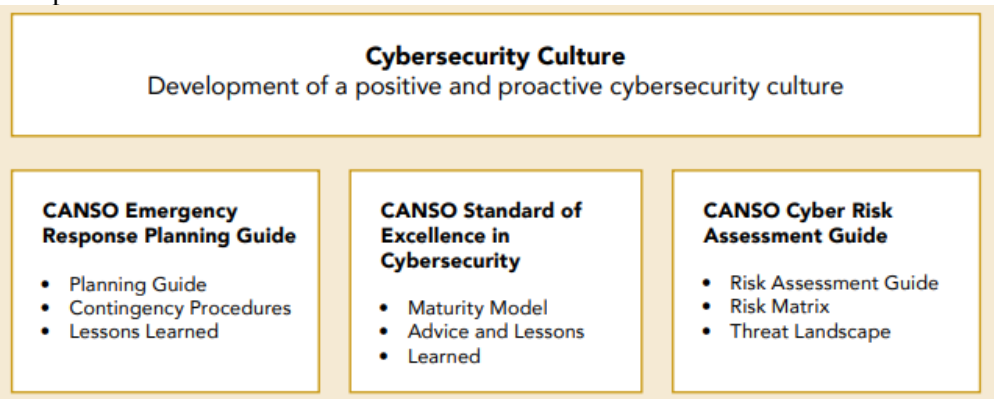
1. INTRODUCTION

1.1 During the 12 December 2024 Ad Hoc Experts Group meeting, it was suggested that the CANSO Standard of Excellence in Cyber Security could be a good document for the CRV OG to review and potentially adopt.

2. DISCUSSION

2.1 The CANSO Standard of Excellence in Cyber Security is a document freely available from the CANSO website.

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



2.3 The Standard of Excellence (SoE) contains the cybersecurity maturity model to enable an Air Navigation Service Provider (ANSP) to assess its own as well as their suppliers' cybersecurity maturity. The maturity model comprises thirteen elements based on six functions that would be expected in an organisation with an effective approach to cybersecurity.

2.4 Each element is described in detail in the maturity model, with five different levels of maturity ranging from having informal arrangements in place to an optimised approach. The assessment against each element is conducted using a scoring form containing probing questions, which enables an organisation and its supply chain to identify their current level of maturity.

2.5 Some of the document references are:

- ISO 27000
- ISO 27001
- NIST CSF
- ISO 27002
- ISO 27005
- CANSO Cybersecurity and Risk Assessment Guide
- ED-201
- EN 16495
- ICAO doc. 8973 section 18.1.6 (RESTRICTED)
- ICAO doc. 9985 Appendix B section 3.2 (RESTRICTED)

2.6 The document is very similar to the NIST CSF framework but on a smaller scale. It covers the following themes:

- Lead and Govern
- Identify
- Protect
- Detect
- Respond
- Recover

2.7 An example output is provided in the document as below.

Function	Capability	ANSP	Supplier 1	Supplier 2	Supplier 3	Supplier 4	Supplier 5
Lead and Govern	Leadership and Governance	D	D	D	C	B	B
	Information Security Management System	C	D	C	C	C	B
Identify	Asset Management	E	E	D	C	C	B
	Risk Assessment	B	D	D	B	C	B
	Information Sharing	C	D	C	B	B	A
	Supply Chain Risk Management	C	D	D	C	B	A
Protect	Ident ity Management and Access Control	D	E	C	C	D	C
	Human - Centred Security	B	D	D	C	C	A
	Protective Technology	D	E	C	D	B	B
Detect	Anomalies and Events	D	C	C	C	C	A
Respond	Response Planning	C	D	D	D	A	A
	Mitigation	D	D	C	C	A	B
Recover	Recovery Planning	D	D	D	B	C	B

2.8 The idea is to first agree a maturity level that is acceptable and then to carry out the maturity assessment. Once the assessment has been carried out, a plan is created to improve any score that is below the agreed acceptable level.

2.9 Using CANSO Standard of Excellence in Cyber Security to assess the CRV, the result looks like the below.

	CRV OG CANSO SoE Maturity Assessment	Target Score	Assessed Score
	Element		
LEAD AND GOVERN	Leadership and Governance	C	A
	Information Security Management System (ISMS)	C	A
IDENTIFY	Risk Assessment	C	A
	Information sharing	C	A
	Supply Chain Risk Management	C	A
PROTECT	Identity Management and Access Control	C	B
	Human Centred Security	C	A
	Protective Technology	C	B
DETECT	Anomalies and Events	C	B
RESPOND	Response Planning	C	B
	Mitigation	C	A
RECOVER	Recovery Planning	C	A

2.10 The following Decision, is expected from the meeting.

Draft Conclusion CRV OG/13/xx Adopt the CANSO Standard of Excellence in Cyber Security	
What: The CRV OG recommends the CANSO Standard of Excellence in Cyber Security and: a) Agrees on an acceptable maturity level. b) Carries out the maturity assessment on the CRV. c) Request that PCCWG also carry out the maturity assessment. d) Request each state to carry out the maturity assessment. e) Create a plan to address the gaps in the maturity score for the CRV.	Expected impact: ☐ Political / Global ☐ Inter-regional ☐ Economic ☐ Environmental ☒ Ops/Technical
Why: To have a standard Cyber Security maturity applied to the CRV.	Follow-up: ☒Required from States
When: 8-Mar-25	Status: Draft to be adopted by Subgroup
Who: ☒Sub groups ☒APAC States ☒ICAO APAC RO ☐ICAO HQ ☐Other: XXXX	

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information contained in this paper;
b) deliberate proposal for using CANSO Standard of Excellence in Cyber Security to assess the CRV;
c) endorse the proposed draft conclusion; and
d) discuss any relevant matter as appropriate

– – – – – – – – – – – – –