International Civil Aviation Organization

THE FIFTEENTH MEETING OF THE COMMON AERONAUTICAL VIRTUAL PRIVATE NETWORK OPERATIONS GROUP (CRV OG/15)

Mumbai, India, 15-19 June 2026

Agenda Item 12: Cyber-safety/security and resilience

CANSO CYBER SECURITY ASSESSMENT OF CRV

(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 Fourteenth CRV OG Ad Hoc Experts Group Meeting on 12 December 2024, 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.

1.2 This was presented at CRV OG 13 in Wellington, New Zealand, 03-08 March 2025 by WP/26, with an initial assessment of A or B on a scale of A to E, where E is the highest level.

1.3 CRV OG/13 endorsed the **Draft Conclusion CRV OG/13/07- Adopt the CANSO Standard of Excellence in Cyber Security** for ACSICG/12 adoption, which was endorsed by the ACSICG/12 Meeting (25-28 March 2025).

1.4 The CANSO Standard of Excellence in Cyber Security, endorsed by ACSICG/12 for adoption of CNS SG/29, was adopted by CNS SG/29 with **slight changes in the title and body** of the conclusion to clarify that **the proposed framework is recommended for the CRV network only.**

Conclusion CNS SG/29/02 *(Draft Conclusion ACSICG/12/03 (CRV OG/13/07))*- Adopt the CANSO Standard of Excellence in Cyber Security for CRV	
What: The CRV OG adopts the CANSO Standard of Excellence in Cyber Security for CRV and recommends that: a) CRV OG prefers an acceptable maturity level of Target Score 'C.' in carrying out the maturity assessment on the CRV. b) The CRV Service Provider carries out the maturity assessment. c) Each participating State/Administration carries out the maturity assessment.	Expected impact: ☐ Political / Global ☐ Inter-regional ☐ Economic ☐ Environmental ☒ Ops/Technical

d) CRV OG/Each participating State/Administration creates a plan to address the gaps in the maturity score for the CRV.		
Why: To have a standard Cyber Security maturity applied to the CRV.	Follow-up:	☒Required from States
When: 20-Jun-25	Status:	Adopted by Subgroup
Who: ☒Sub groups ☒APAC States ☒ICAO APAC RO ☐ICAO HQ ☐Other: CRV OG		

1.5 The CRV OG/13 Meeting noted that many States/Administrations have their own cybersecurity framework and standards to follow. However, it was agreed that the proposed maturity assessment for the CRV is neither time-consuming nor challenging, and it was recommended that all CRV users conduct it. The ACSICG/12 Meeting discussed concerns about further actions for States/Administrations whose maturity assessment on the CRV is below the **Target Score 'C.'** It was recommended that **CRV OG create guidelines for the next steps in these cases,** including associated timelines to achieve Target Score 'C'.

1.6 This paper shares the assessment done by New Zealand for the CRV network using the CANSO Standard of Excellence in Cyber Security.

2. DISCUSSION

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

2.2 There 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 agreed maturity level for CRV is Level C – Managed. Using the CANSO Standard of Excellence in Cyber Security to assess the CRV, the result for New Zealand in 2025 is as follows.

	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
IDEN TIFY	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

2.9 For 2026, the assessment is very similar.

Improvements have been made in Risk Assessment, Supply Chain Risk Management, Identity Management and Access Control, Protective Technology, Mitigation and Recovery Planning.

	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	B
	Information sharing	C	A
	Supply Chain Risk Management	C	B
PROTECT	Identity Management and Access Control	C	C
	Human Centred Security	C	A
	Protective Technology	C	C
DETECT	Anomalies and Events	C	B
RESPOND	Response Planning	C	B
	Mitigation	C	B
RECOVER	Recovery Planning	C	B

2.10 Due to the nature of the CRV OG, limited improvements can be made; however, there are opportunities to be made in **Anomalies and Events and Response Planning** through the Ad Hoc group.

3. ACTION BY THE MEETING

3.1 The Meeting is invited to:

a) note the information contained in this paper;

b) note the assessment conducted by Airways New Zealand;

c) encourage States/Administrations to conduct such an assessment for CRV; and

d) discuss any relevant matter as appropriate.

– – – – – – – – – – – – –