

CANSO activities on Cybersecurity

Tanja Grobotek
CANSO Director Europe Affairs

ICAO EUR/NAT DGCA

10 May 2022

About CANSO

WE ARE THE VOICE OF AIR TRAFFIC MANAGEMENT



180
Members



86
ANSPs

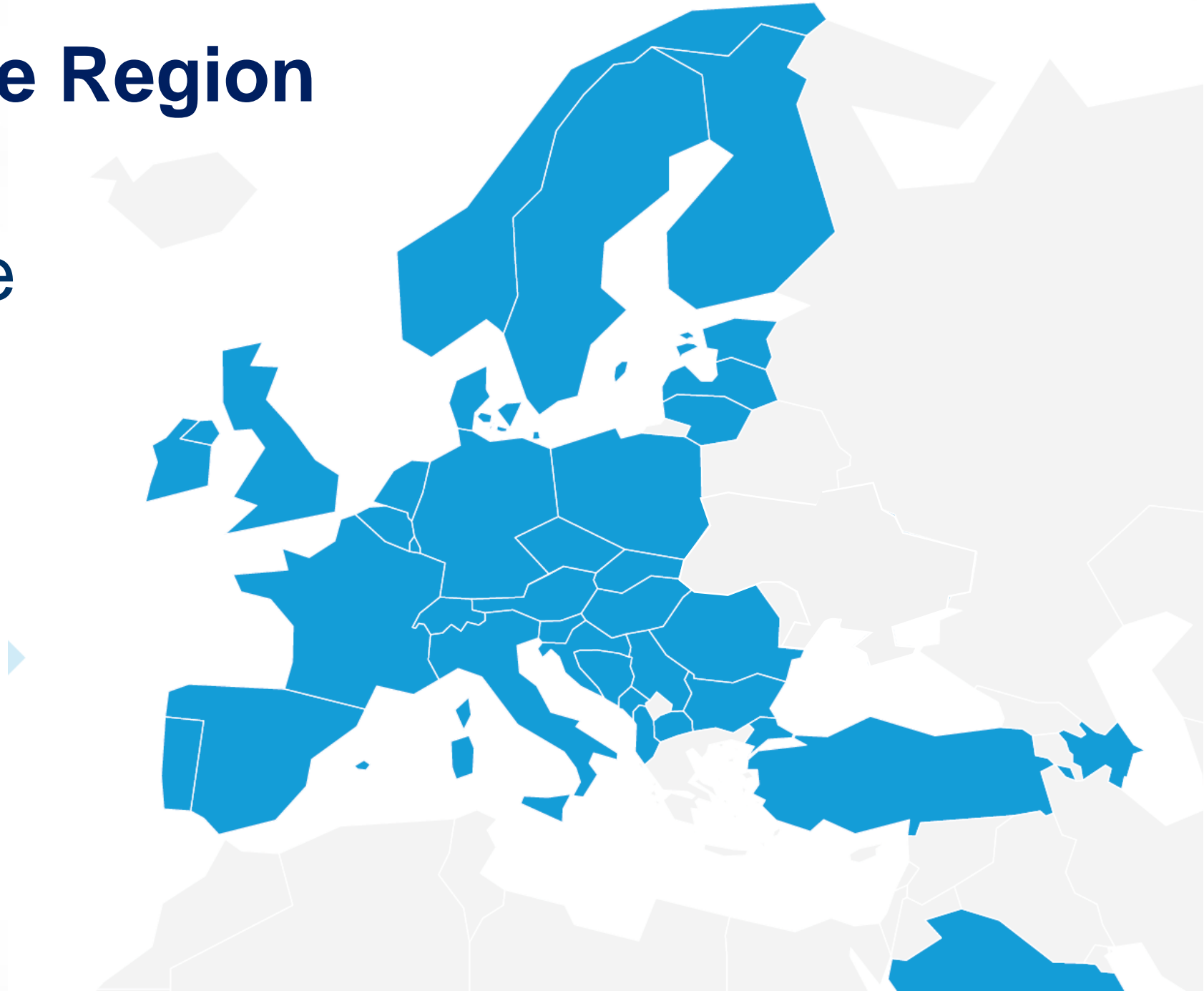


94
Technology and other service
providers

CANSO Europe Region

CANSO Europe
Members:

35 ANSPs



CANSO Standard of Excellence in Cybersecurity

The CANSO Standard of Excellence in Cybersecurity supports ANSPs by:

- Highlighting the critical elements of effective cybersecurity
- Allowing comparison of maturity levels either internally or externally, providing accessible, high-level summaries for management
- Facilitating a harmonised approach to cybersecurity across the ATM industry.



CYBERSECURITY EFFECTIVENESS

CYBERSECURITY MATURITY

E

Level E – Optimised

Cybersecurity processes and/or requirements set international best practice, focusing on innovation and improvement. Feedback and improvement are embedded in the organisation. The effectiveness of the cybersecurity improvement actions is measured and evaluated against defined improvement criteria.

D

Level D – Assured

Evidence is available to provide confidence that cybersecurity processes and/or requirements are being applied appropriately and are delivering positive, measured results.

C

Level C – Managed

Cybersecurity processes and/or requirements are formally documented and consistently applied.

B

Level B – Defined

Cybersecurity processes and/or requirements are defined but not yet fully implemented, documented or consistently applied.

A

Level A – Informal Arrangements

Cybersecurity processes and / or requirements have not been agreed at the organisation level - they are either not routinely undertaken or depend on the individual assigned to the task.

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	Identity 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

Other CANSO Global Cybersecurity Activities

CANSO Emergency Response Guide

- The Guide helps ANSPs develop a formal emergency response plan that documents the orderly and efficient transition from normal to emergency operations and return to normal operations.

Cybersecurity Maturity Model (with EUROCONTROL)

Contribution to ICAO activities

- Observer – Cybersecurity Panel (CYSECP)
- Member of the Trust Framework Study Group

Cybersecurity in Europe

Information Security is now explicitly considered, by different international and European legislations, as a binding requirement considering the need to protect both critical infrastructures in general and the Civil Aviation systems and information in particular.

Main Priorities:

- Contribute to the European Union regulatory/oversight framework in the field of information security
 - European Strategic Coordination Platform (ESCP)
 - EU Cybersecurity Strategy
 - 'Management of information security risks' (Part-IS) & GM/AMC
- Support harmonised implantation of NIS Directive, Regulation 2017/373
- Share best practices
- Monitor Standardization activities (ECSCG, EUROCAE, CEN, ECAC, ECTRL)

TEMPLATE OF CYBER SECURITY REQUIREMENTS FOR USE IN THIRD PARTY CONTRACTS

This template document makes available a series of common security requirements which may be used by CAN SO Europe and Borealis Alliance members when undertaking tendering processes in relation to operational products and services. The benefit of this document to the members is that, when presented to manufacturers and/or service providers at the earliest possible stage, these requirements may be considered and costed as initial requirements rather than as ‘add-on features’ as described by manufacturers/service providers which often result in an extra, increased cost.

The requirements have been set at a level that is not excessively technical but instead suitably high-level, thereby allowing the vendors to use their own skills and capabilities to establish the methods by which the requirements are met. Ultimately it will be for the customer to assess whether their requirements have indeed been met; this flexibility remains the right of the customer although this template will serve as the benchmark against which that assessment may be made.

The template document recognises that in some instances there will not be a clear basis upon which certification from an Internationally recognised Standardisation Body can be achieved. In order to support customers in this situation, a list of standards is included which may allow suppliers and/or service providers to demonstrate the existence of acceptable processes, practices, and procedures.

The template itself is considered to be a “living” document which will adapt and change through use in order to continually reflect best practice and experience.

CAN SO Key messages

- The current increase in geopolitical tensions has caused significant overhead and concerns amongst ANSP's because of our reliance on global digital interconnectivity. There is an urgent need to improve and support work under ICAO to improve our digital resilience.
- ANSP information sharing and cooperation should improve to deal with common threats and risks.
- We should consider common approaches towards security architecture and managing the supply chain, which would deliver efficiency and effectiveness benefits.

The Complete Air Traffic System (CATS) Global Council

Our Shared Vision for 2045

A Blueprint for Future Skies



2045 Vision Building Blocks



Services and Service Delivery



Technology and Digitisation



Safety and Regulation



Environmental Sustainability and Social Impact



Airspace Design and Classification



Data and Security



People, Organisation and Talent



THANK YOU

CANSO

SHAPING OUR FUTURE SKIES