
ICAO • OACI • ИКАО
国际民航组织 • ايكاو
INTERNATIONAL
CIVIL AVIATION
ORGANIZATION

Cybersecurity in Air Navigation Services

Threats, Standards, Resilience

Technical and Operational Briefing for ANSP Staff

Mayda Alicia Ávila
Regional Officer, Communications, Navigation and Surveillance (CNS)
International Civil Aviation Organization North American, Central American and Caribbean Regional Office

Why ANS Is a Target

- Digitalisation and interconnection across air traffic management have widened the exposure of air navigation services to cyber risk.
- Impacts range from minor delays to catastrophic loss of safety, security and service continuity.
- The long-held assumption of isolated, specialist networks no longer holds as next-generation systems interconnect. Aviation has seen incidents but no truly disruptive cyber event — a record that may owe as much to luck as to design.

ICAO | OACI

The ICAO Framework

Standards and Resolutions

- ICAO's response has built up over two decades: Doc 9985 ATM Security Manual (2013), then the first cybersecurity Standard in Annex 17 (2016).
- Assembly Resolution A39-19 recognised cybersecurity as core to civil aviation. A40-19 introduced the Aviation Cybersecurity Strategy and urged adoption of the Beijing Convention and Protocol.
- A41-19 calls on States to implement the Cybersecurity Action Plan and designate a competent cybersecurity authority.

ICAO Assembly	Resolution	Year	Title / Main significance
39th Assembly	**A39-19**	2016	**Addressing Cybersecurity in Civil Aviation** — First dedicated ICAO Assembly Resolution establishing cybersecurity as a global civil aviation priority.
40th Assembly	**A40-10**	2019	**Addressing Cybersecurity in Civil Aviation** — Superseded A39-19. Strengthened the global framework and called for implementation of the **ICAO Aviation Cybersecurity Strategy** and development of the **Cybersecurity Action Plan (CyAP)**.
41st Assembly	**A41-19**	2022	**Addressing Cybersecurity in Civil Aviation** — Superseded A40-10. Reinforced governance, cooperation, risk management, cybersecurity culture, implementation of the Strategy/CyAP, and adoption of the Beijing legal instruments.
42nd Assembly	**A42-19**	2025	**Addressing Cybersecurity in Civil Aviation** — **Current/latest Resolution**, superseding A41-19. Continues ICAO's holistic approach linking cybersecurity with aviation **safety, security and efficiency**, and emphasizes governance, international cooperation and implementation.

The ICAO Cybersecurity Strategy

International cooperation

- States, ANSPs and industry must share information, harmonise regulation and coordinate response.
- Civil-military coordination and trust frameworks are essential.

Governance and cybersecurity policy

- States must assign clear accountability for aviation cybersecurity through a competent national authority.
- Cybersecurity must be integrated into security and safety programmes, with risk managed across the full system lifecycle.

Legislation, regulation and information sharing

- Adopt law enabling deterrence, investigation and prosecution of cyber attacks; use trusted platforms and the Traffic Light Protocol for disclosure.
- Incident management and capacity building: scalable contingency plans, live cyber exercises, training and a cybersecurity culture underpin delivery through the Cybersecurity Action Plan.

Annex 17 and Doc 9985

Standard 4.9.1

- Entities under the national civil aviation security programme must identify critical ICT systems and data and protect them on a risk-management basis.
- Recommended Practice 4.9.2 addresses confidentiality, integrity and availability through security by design, supply-chain security, network separation and controlled remote access.
- Doc 9985 extends this to ATS facilities and CNS infrastructure — people, procedures, information, facilities and equipment.

The Standards

- ISO/IEC 27001 sets the requirements for an information security management system and is the certifiable core of the series, supported by 27002 controls, 27005 risk management, 27031 ICT readiness for business continuity, 27033 network security and 27035 incident management.
- ISO 31000 supplies the generic risk framework and IEC 62443 covers industrial control systems.
- Certification evidence also supports USOAP CMA audits and Annex 17 and Annex 19 obligations.

Cybersecurity assessment based on:

- ICAO Cybersecurity Action Plan
- ICAO Cybersecurity Policy Guidance
- ICAO Document 8973 “Aviation Security Manual”
- ICAO-CANSO-AIRBUS “Air Traffic Management Cybersecurity Policy Template”
- ICAO Annex 17, 19
- CANSO Cybersecurity Risk Assessment Guide
- ICAO Document 10213 Global Cyber Risk Codirections
- ACI - Cybersecurity for Airports Executives Handbook
- ISO Standards 27000, 31000
- NIST SP 800-30 is a U.S. National Institute of Standards and Technology (NIST)
- EUROCAE (European Organization for Civil Aviation Equipment) and RTCA “Guidance on Aviation Cybersecurity”

OACI

The ATM Attack Surface

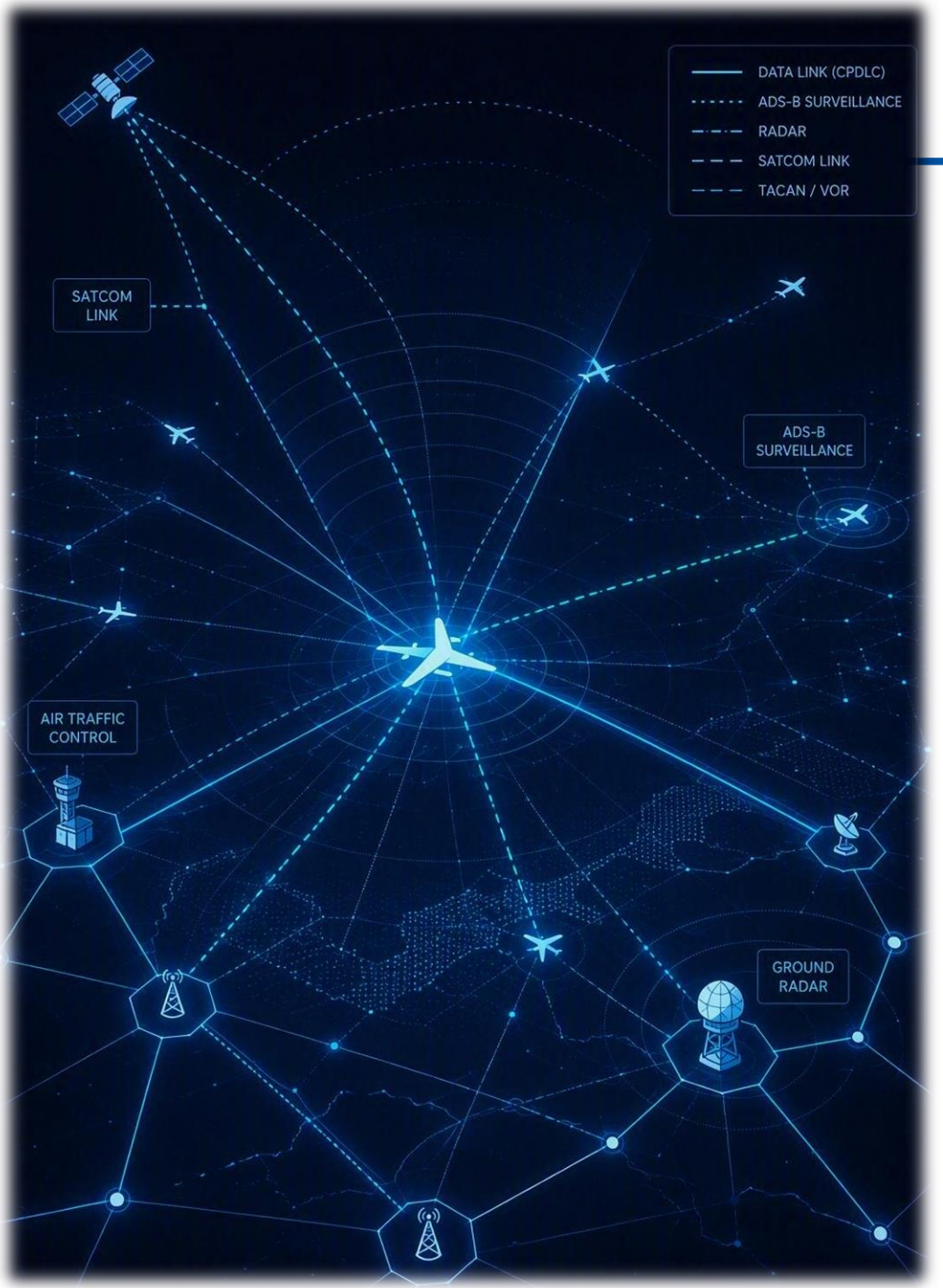
Surveillance: ADS-B, multilateration and radar depend on broadcast data that can be spoofed or jammed.

Navigation: GNSS interference and spoofing, mitigated through VOR/DME minimum operational networks and SBAS/GBAS integrity monitoring.

Communications: CPDLC, VHF and SATCOM links plus regional ATM data networks such as MEVA, REDDIG and CANSNET.

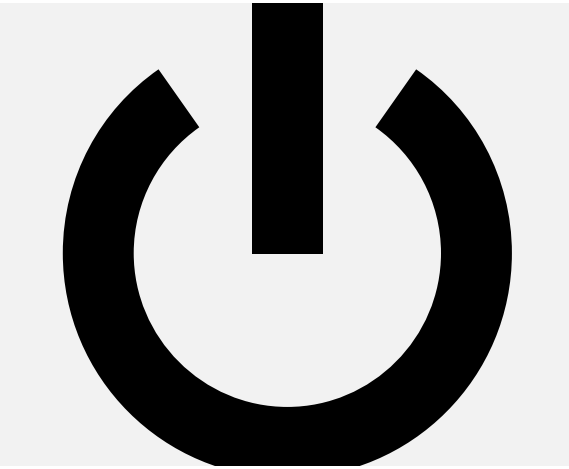
Information systems: AIM, FF-ICE, MET and flight-plan data exposed to alteration and unauthorised access.

Infrastructure and partners: IT, OT and industrial control systems, together with every interconnection to external stakeholders.



OACI

Threat Landscape for ATM (Doc 10213)



Availability

- Ransomware.
- Distributed denial of service.
- Power and HVAC degradation.
- Loss of IP connectivity.

Integrity

- Falsified MET, flight plan and surveillance data.
- GNSS spoofing.

Confidentiality

- Theft of intellectual property and data.
- Ransomware exfiltration.

Assessing the Risk

A defined process: ISO 31000 sets scope, context and criteria, then identification, analysis, evaluation, treatment, monitoring and reporting.

Applied to ATM: ISO/IEC 27005 lets ANSPs assess surveillance attacks, GNSS interference and denial of service against ATC voice and data.

Intelligence-led: Assessment must be threat-focused and embedded in the system lifecycle rather than run as a periodic paper exercise.

Clear ownership: Every ATM asset — data, systems and personnel — requires a defined owner accountable for its protection.

No common point of vulnerability: Mirror the safety principle of no single point of failure across the security architecture.

The Doc 9985 Control Library

Nine control categories

- Policy direction; organisation, culture and management; human resources; physical and environmental security; ICT operations; technical mechanisms and infrastructure; acquisition and development; supervision and audit; and compliance.

Protecting availability

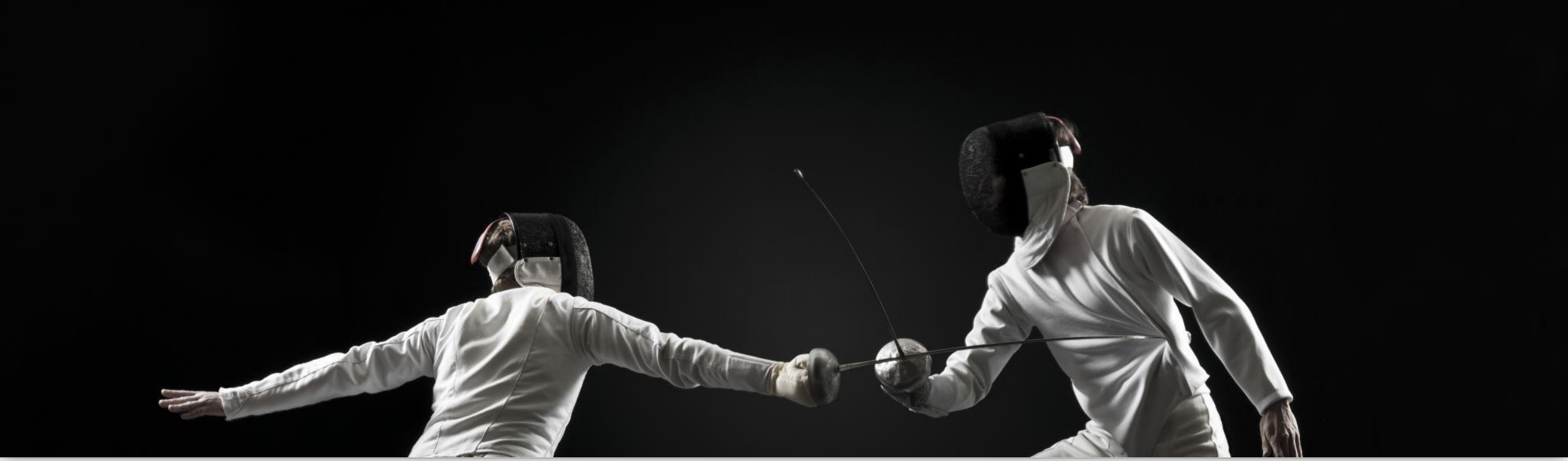
A managed continuity process, service level agreements, capacity monitoring, tested backups and offsite storage.

Protecting integrity

- Safeguards for data in transit against alteration, misrouting and duplication, reinforced by validation checks.

Protecting confidentiality

- Information classification, non-disclosure agreements, routing controls and leak-prevention mechanisms.



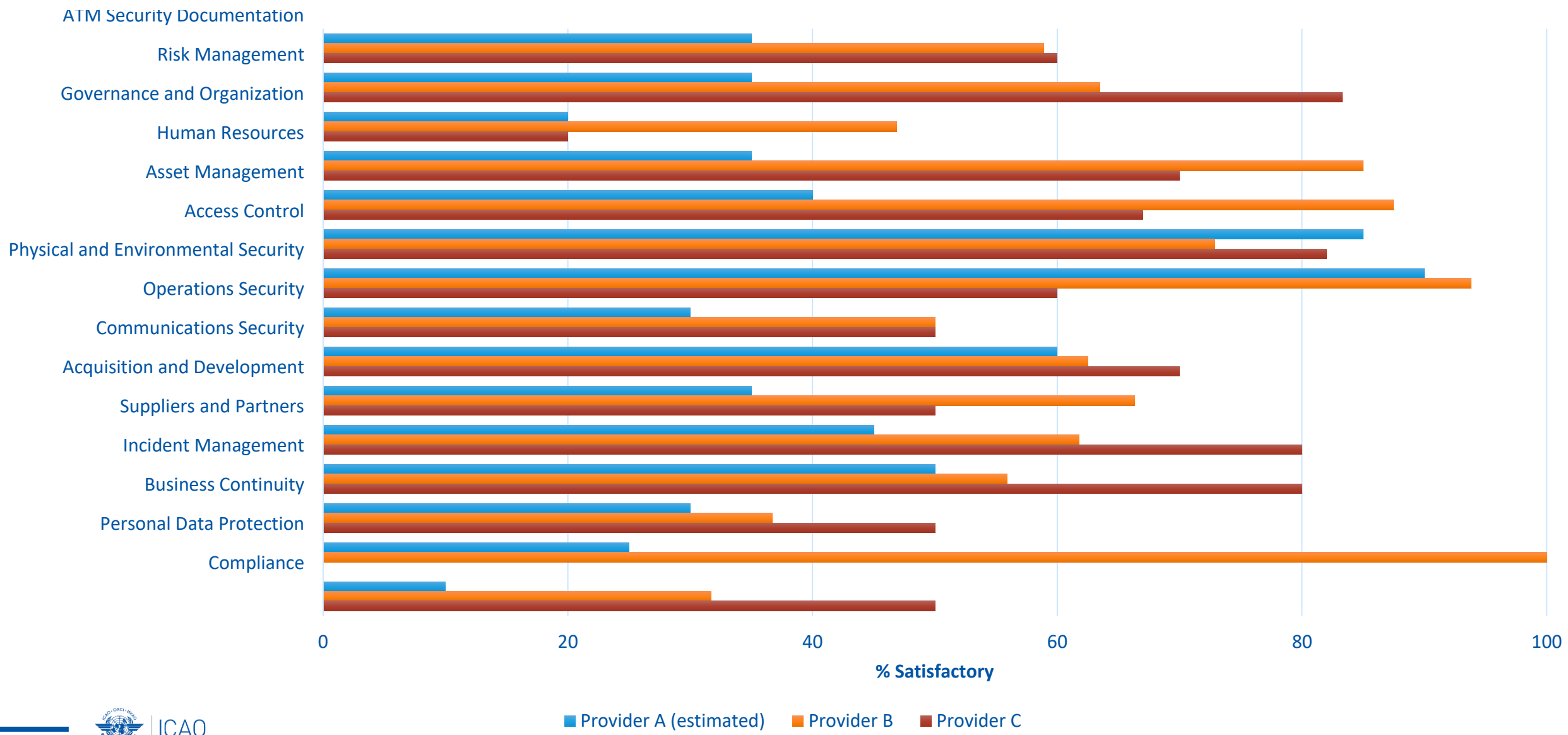
Business Continuity

- No defence is perfect; cost and resource limits force trade-offs, so an incident remains possible.
- Annex 11 requires ATS authorities to prepare and promulgate contingency plans coordinated with adjacent FIRs.
- Plan for site recovery, system recovery and operational continuity against defined recovery times.

Self-Assessment

- The ANSP cybersecurity checklist lets a provider assess itself against the ATM Cybersecurity Policy Template across fifteen domains.
- Domains run from documentation, risk management and governance through access control, physical security of CNS/ATM, operations, suppliers, incident management and business continuity to compliance.
- Scope covers TWR, APP and ACC units, CNS infrastructure and digital AIM and MET systems, with each item mapped to ISO/IEC 27001:2022 clauses and Annex A controls.

Evaluation Results Across Three Providers



Provider A was assessed qualitatively; its values are estimated from narrative findings. Overall maturity: Provider B 64.9%, Provider C approx. 58%.

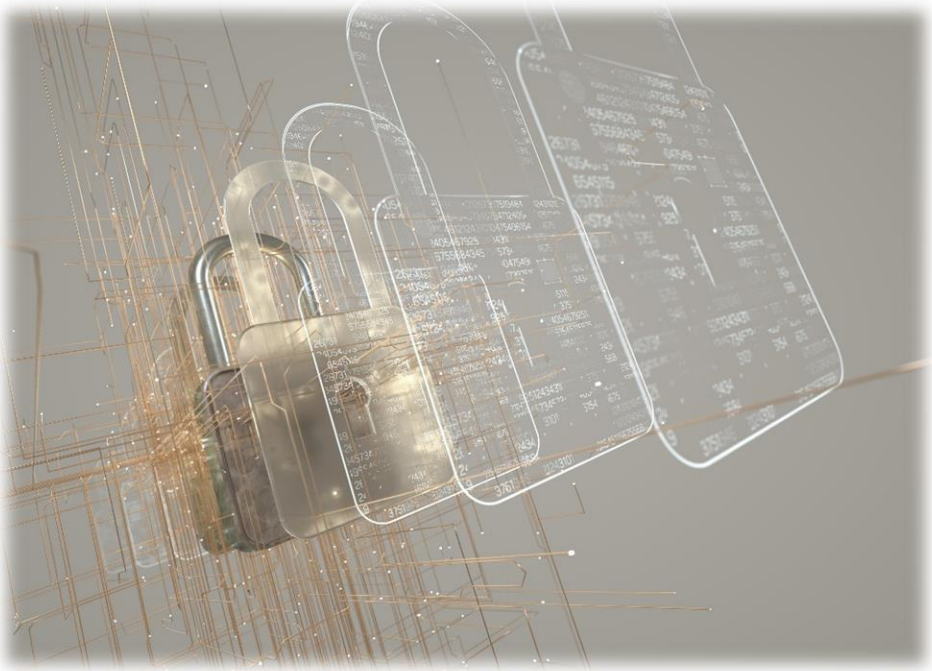
Strengths

- Access control well managed across physical, logical and administrative layers
- Robust physical and environmental security of CNS/ATM facilities
- IT/OT network segmentation and trust zones effectively implemented
- Asset management and human resources practices generally established
- Cybersecurity included in staff onboarding and routine awareness communication

Weaknesses

- No formal cybersecurity governance framework or defined individual accountability
- Operations security gaps: no continuous monitoring, vulnerability or patch management
- Business continuity not linked to cyber risk; no BIA, untested backups, no exercises
- Compliance and independent audit the weakest domain across all three providers
- Supplier and third-party security not formally managed or audited
- Incomplete asset inventories, especially OT and remote sites

Governance and Next Steps



*The ATM Cybersecurity Policy Template, developed by ICAO NACC with CANSO and Airbus, calls on providers to establish a **risk-based management system** with senior-management commitment, clear roles and State oversight independent of the provider.*

*For ATM staff the next steps are practical: **run the checklist, prioritise gaps by risk, exercise the contingency plans, and join trusted information-sharing mechanisms**.*


ICAO
Headquarters
Montréal
European and
North Atlantic
(EUR/NAT) Office
Paris
Asia and Pacific
(APAC) Sub-office
Beijing
Middle East
(MID) Office
Cairo
Western and
Central African
(WACAF) Office
Dakar
North American
Central American
and Caribbean
(NACC) Office
Mexico City
Asia and Pacific
(APAC) Office
Bangkok
Eastern and
Southern African
(ESAF) Office
Nairobi
South American
(SAM) Office
Lima

Thank you