Cybersecurity Action Plan

Published by authority of the Secretary General

Second edition, January 2022

International Civil Aviation Organization

Terms and definitions[1]

caISMS: civil aviation Information Security Management System

A model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the protection of information assets to achieve civil aviation objectives based upon a risk assessment and the organization's risk acceptance levels designed to treat and manage risks. Source ISO27000:2009.

Cybersecurity

The body of technologies, controls and measures, and processes and practices designed to ensure confidentiality, integrity, availability and overall protection of systems, networks, programmes, devices, information and data from attack, damage, unauthorized access, use and/or exploitation.

Cybersecurity Policy

A cybersecurity policy documents the intentions and direction of an organization, for the management of cybersecurity threats, as expressed by top management. It is a written document in an organization outlining how to protect the organization from cybersecurity threats, and how to handle incidents and events when they do occur.

Event

Identified occurrence in a system, service or network state indicating a possible breach of information security policy or failures of control, or a previously unknown situation that may be security relevant [ISO/IEC 27035]. It shall be noted that 'occurrence' needs to be considered in its broad sense and shall not be understood as (safety) occurrence term that only embraces the events which have, or could have, significance in the context of aviation safety.

Incident

Single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security [ISO/IEC 27035-1]

Information Security

Preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can be involved. [BS ISO/IEC 27000:2018]

Information Sharing

The process through which information is provided by one entity to one or more other entities to facilitate risk-based decision-making and promote best practices.

Risk matrix

Tool for ranking and displaying components of risks (threat, likelihood, impact/consequence, and vulnerability), risk mitigation measures implemented, *and, ultimately, the residual risks.*

Threat entity (or actor)

Entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact – an organization or system.

---

[1] Still under review

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat entity. This may be a system which directly or indirectly supports a function of the aviation system.

EXECUTIVE SUMMARY

The 39th Session of the International Civil Aviation Organization (ICAO) Assembly reaffirmed the importance and urgency of protecting civil aviation's critical infrastructure systems and data against cyber-attacks, and obtaining global commitment for action by ICAO, its Member States and industry stakeholders, with a view to collaboratively and systemically addressing cybersecurity in civil aviation and mitigating the associated threats and risks. Resolution A39-19 – *Addressing Cybersecurity in Civil Aviation* identified the actions to be undertaken by States and other stakeholders in this regard. The 39th Session of the ICAO Assembly also instructed ICAO to develop a comprehensive cybersecurity work plan.

In order to meet the expectations of the Assembly, a Cybersecurity Strategy for civil aviation was developed by the Secretariat Study Group on Cybersecurity (SSGC).

The 40th Session of the ICAO Assembly adopted the amended Resolution A40-10 – *Addressing Cybersecurity in Civil Aviation*, which calls upon States to implement the Cybersecurity Strategy and underlines the importance of developing a sustainable implementation plan for the Strategy, as well as continuing the work for the development of a strong cybersecurity framework.

The Cybersecurity Action Plan (CyAP) provides the foundation for States, industry, stakeholders and ICAO to work together to develop the ability to identify, prevent, detect, respond to and recover from cyber-attacks on civil aviation as well as create a solid framework for cooperation. It has been developed with the aim to propose a series of principles, measures and actions to achieve the objectives of the strategy's seven pillars.

Chapter 1

INTRODUCTION

1.1 BACKGROUND

1.1.1 In the current civil aviation context, air traffic is projected to increase over the long term, technology evolves swiftly, operations are becoming more complex, and the operational environment consequently becomes more challenging. Rapid technological changes are altering the way civil aviation operates and making the system more vulnerable to cybersecurity threats. Malicious cyber activity can affect civil aviation in a variety of ways, from a small disruption of operations to catastrophic outcomes. Risks are growing rapidly and there is a strong need for a sustainable cybersecurity framework at the international, regional and national levels.

1.1.2 Building a robust cybersecurity infrastructure, which relies on strong cooperation among States, industry, and ICAO, enables the creation of a common cybersecurity awareness that will ultimately lead to a more secure and resilient civil aviation system.

1.1.3 ICAO is constantly adapting to meet the ever-evolving global threat picture, in line with the United Nations Security Council's resolutions that affirm States' responsibility to ensure the safety of air services operating within their territory and call upon all States to work with ICAO to ensure that international security standards are reviewed, updated, and put in place, based on current risks, pursuant to the Chicago Convention. As cybersecurity threats to civil aviation are evolving and will likely increase in prevalence, following the provisions of UNSCR 2341 (2017), ICAO is focused on establishing appropriate mechanisms to mitigate and reduce risks to aviation critical infrastructure from unlawful interference through cyber vectors and from any event that may impact the safety of operations.

1.1.4 In this respect, in order to properly achieve the objectives of the seven pillars of the Aviation Cybersecurity Strategy and to shape a cybersecurity framework, this Action Plan has been developed.

1.2 PURPOSE

1.2.1 This Plan is a living document that will evolve with developments in cybersecurity and will be regularly updated to reflect the required changes stemming from, among other things, the gap analysis and activities described in Chapters 3 and 4. The CyAP captures the objectives and actions to be achieved for the implementation of the ICAO Aviation Cybersecurity Strategy. The elements presented in this document reflect the work done or that is currently ongoing within different regions/States or industry. It encompasses the results of analysis of the current "as-is" situation of the aviation system from a cybersecurity perspective, when compared to the "to-be" situation proposed in the strategy, elaborating on an action plan that can drive such evolution towards the strategic vision.

1.2.2 Given the significant work required in implementing the objectives and actions set out in this document, a staged approach, identifying short, medium and long-term targets, is proposed in Appendix A.

1.3 RISK CONTEXT

1.3.1 Cybersecurity is not a new concept in civil aviation. However, as cybersecurity threats have become increasingly prevalent, it has become one of the centrepieces when discussing and analysing risks to and vulnerabilities of the civil aviation system. The civil aviation sector is particularly at risk, because cyber-attacks are more likely to be successful in a sector in which components are growing in a functionally and digitally interdependent way, and also because the cyber-defence mechanisms currently in use by the civil aviation sector are not yet adequate to deal with this persistent and adaptive threat.

1.3.2 The ICAO Aviation Security Panel most recently evaluated the level of risk stemming from the exploitation of a vulnerability, in a terrorist context, as medium. This assessment is based on residual vulnerability in the cybersecurity field, assuming that States have effectively implemented Annex 17 – *Security* provisions. However, cyber risks are rapidly evolving and they must be assessed for all cyber-attacker profiles that could affect not only security but also safety of civil aviation operations. Furthermore, the source of cyber-attacks is often difficult to trace, and, as such, attribution and prosecution of cyber-attacks is often complicated and difficult to accomplish, while leaving the victim of the attack or their insurers to bear the recovery costs. For these reasons, it is of extreme importance that ICAO, States and industry work collaboratively to implement the Cybersecurity Strategy in a systematic manner.

1.4 BENEFITS OF THE ACTION PLAN

1.4.1 The CyAP aims at ensuring the commitment of ICAO, Member States, and industry to implement the Aviation Cybersecurity Strategy and achieve the objectives outlined in its seven pillars. A strong cybersecurity framework will strengthen the civil aviation system and will be beneficial to the entire global aviation community.

Chapter 2

OBJECTIVE

2.1 OBJECTIVE OF THE CYBERSECURITY ACTION PLAN

2.1.1 The goal of the Cybersecurity Action Plan is to achieve the objectives outlined in each of the seven pillars of the Cybersecurity Strategy, as well as the development of a robust civil aviation cybersecurity framework.

2.1.2 The principles that form the foundation of the present Action Plan are:

a) understanding by Member States of the obligations they have with respect to cybersecurity deriving from the *Convention on International Civil Aviation* (Chicago Convention) to ensure the safety, security and continuity of civil aviation operations;

b) coordination of aviation cybersecurity measures amongst Member State authorities to ensure effective and efficient global management of aviation cybersecurity; and

c) commitment of all civil aviation stakeholders to further develop cyber-resilience and protect aviation against cyber-attacks, originating from whatever threat actor profile, that might impact safety, security and continuity of the air transport system.

2.2 APPLICATION

2.2.1 This document is primarily targeted at ICAO Member States and industry, as a means to assist them in managing cybersecurity risks in civil aviation, through a comprehensive, coordinated and holistic approach.

2.2.2 States, industry and other relevant stakeholders should undertake the actions stemming from this action plan.

Chapter 3

STRATEGIC ACTION PLAN

3.1 THE SEVEN PILLARS OF THE AVIATION CYBERSECURITY STRATEGY

3.1.1 The elements documented in this chapter have been developed with the aim to propose a series of principles, measures and actions to achieve the objectives of the Aviation Cybersecurity Strategy's seven pillars, namely:

1. International cooperation
2. Governance
3. Effective legislation and regulations
4. Cybersecurity Policy
5. Information sharing
6. Incident management and emergency planning
7. Capacity building, training and cybersecurity culture

PILLAR 1 - INTERNATIONAL COOPERATION
• Develop cooperation at the national and international level between all stakeholders. • Recognize mutually the efforts (develop, maintain and improve cybersecurity) to protect civil aviation. • Pursue regulatory harmonization at the global, regional and national level in order to promote global coherence and ensure interoperability of protection measures. • Engage States in addressing cybersecurity in international civil aviation. • Facilitate and promote international events in the cybersecurity field. • Recognize that cybersecurity is a shared responsibility across all segments in the global civil aviation system.

PILLAR 2 - GOVERNANCE
• Encourage, support and build upon the ICAO Cybersecurity Strategy. • Develop clear national governance and accountability for civil aviation cybersecurity. • Ensure coordination at the State level between Civil Aviation authorities and the competent national authorities for cybersecurity. • Establish appropriate coordination channels among various State authorities and industry. • Include cybersecurity in national civil aviation safety and security programmes. • Include cybersecurity in global and regional plans. • Work towards a common baseline for cybersecurity Standards and Recommended Practices.

PILLAR 3 - EFFECTIVE LEGISLATION AND REGULATIONS
• Ensure that international legal instruments provide an appropriate framework for the deterrence of cyber incidents as well as the prosecution of their perpetrators. • Analyze existing national legislation and update or adopt national legislation as necessary to allow for the deterrence, investigation, and prosecution of cyber-attacks which impact the safety, security, efficiency, or continuity of civil aviation. • Ensure that appropriate national regulations and legislation are in place for civil aviation cybersecurity. • Develop appropriate guidelines for States and industry in implementing cybersecurity-related provisions.

PILLAR 4 - CYBERSECURITY POLICY
• Ensure that cybersecurity is part of civil aviation safety and security systems and comprehensive risk management frameworks. • Ensure varying civil aviation cybersecurity risk assessment methodologies retain comparability. • Develop cybersecurity policies considering the complete life cycle of aviation systems.

PILLAR 5 - INFORMATION SHARING
• Develop or leverage existing sharing of information platforms and mechanisms which are recognized, in line with existing ICAO provisions, to enable cyber situational awareness thus allowing prevention, early detection and mitigation of relevant cybersecurity events. • Ensure that any cyber incident or vulnerability which may represent a significant risk to aviation safety and/or security is reported to the competent authority.

PILLAR 6 - INCIDENT MANAGEMENT AND EMERGENCY PLANNING
• Ensure appropriate and scalable plans that provide for the continuity of safe and secure civil aviation operations in case of cyber incidents. • Ensure leveraging existing contingency plans to include provisions to respond to, and recover from, cybersecurity incidents, and regularly/periodically conduct exercises to test the capabilities to detect, respond and recover from cyber incidents.

PILLAR 7 - CAPACITY BUILDING, TRAINING AND CYBERSECURITY CULTURE
• Ensure appropriate role-based qualifications of personnel in both aviation and cybersecurity. • Increase awareness of cybersecurity, including activities to establish appropriate cyber hygiene. • Ensure proper curricula on aviation cybersecurity are included in the national educational framework, in order to ensure the development of a cross aviation safety and security body of knowledge throughout the organization, including its senior management. • Foster cybersecurity innovation and appropriate research and development. • Include cybersecurity in the ICAO Next Generation of Aviation Professionals' strategy.

Chapter 4

IMPLEMENTATION, MONITORING AND REVIEW

4.1 IMPLEMENTATION

The CyAP is targeted to ICAO, its Member States, industry and other stakeholders. Each entity is encouraged to adopt the targets based on the Roadmap (see Appendix A), which outlines priority outcomes, actions and related tasks. This will help ICAO, States, and stakeholders focus and work towards implementing effective measures and actions to achieve the objective of developing a robust global aviation cybersecurity framework.

4.2 MONITORING AND REVIEW

ICAO will conduct a review of the CyAP as and when appropriate. ICAO will also provide status updates for targets and intended deadlines as outlined in the CyAP. These will include areas where States need assistance with the implementation of the CyAP and/or where capacity-building assistance is needed, and other relevant efforts.

4.3 WORKING IN PARTNERSHIP

All aviation stakeholders need to be involved in the effort for the continuous improvement of cybersecurity in civil aviation. The CyAP provides a common frame of reference for all stakeholders and identifies actions that ICAO, Member States, and industry need to take in order for a common cybersecurity framework to be developed.

4.4 ROLE OF ICAO, STATES AND STAKEHOLDERS

4.4.1 ICAO will have an important global leadership and monitoring role in the implementation and coordination of the CyAP, including:

- updating the CyAP as and when required;
- developing and maintaining Standards and Recommended Practices (SARPs) and Procedures for Air Navigation Services (PANS) supplemented by manuals and other guidance;
- monitoring and reviewing the cybersecurity threat and risk landscape; and
- implementing targeted assistance to address deficiencies in civil aviation cybersecurity.

4.4.2 States and industry also have an important role to undertake in the implementation and effectiveness of the CyAP. States and stakeholders are encouraged to demonstrate year on year improvement in the implementation of the plan.

Chapter 5

INTERNATIONAL COOPERATION

5.1 DEVELOPMENT OF AN INVENTORY OF AVIATION CYBERSECURITY INITIATIVES

5.1.1 An inventory of cybersecurity initiatives will be developed, maintained and made available on the ICAO portal for appropriate audiences. This inventory will compile already existing initiatives and encompass existing aviation initiatives related to cybersecurity at the global, regional or national levels. The inventory will not only consider aviation cybersecurity initiatives but also initiatives whose outcomes are relevant to civil aviation (e.g. cybersecurity in other transport domains or sectors like energy, finance).

5.2 ESTABLISHMENT OF A COMMON GROUND FOR INTEROPERABILITY OF CYBERSECURITY MEASURES AND MANAGEMENT SYSTEMS[2]

5.2.1 Principles and appropriate tools/systems should be put in place by States and industry in order to assure uniform, secure, and interoperable management of information technology/communication systems.

5.2.2 As trust is the basis for effective, uniform and interoperable management of information exchanges, development of the International Aviation Trust Framework facilitating information management and interoperability should be supported; furthermore, policies and procedures should be leveraged to the extent possible by all relevant stakeholders.

5.2.3 Interoperability of cybersecurity measures and management can also be achieved by participation in various forms of international cooperation agreements. A model for such agreements should be developed in order to enable cooperation while respecting applicable privacy, information security, and national security policies. In this respect, the following aspects need to be determined as a baseline for model agreements:

- subject and objective of the agreement;
- the entities that could enter into such agreements;
- roles and responsibilities of those entities; and
- measures that could be used to improve cybersecurity in civil aviation and that are subject to coordination.

5.2.4 The international agreements should have, as their purpose:

- establishing a dialogue amongst stakeholders to discuss means to reduce collective risk and protect national and international civil aviation infrastructure;
- risk reduction and mitigation measures to address cybersecurity threats to civil aviation;
- information exchanges on national civil aviation legislation, national strategies, policies and best practices related to cybersecurity; and
- measures to support cybersecurity capacity building where needed.

[2] Management systems in this context include, but are not limited to, risk management systems.

5.2.5 In a context where many methodological principles and models, as well as a different vocabulary, may exist amongst aviation stakeholders, it is key to develop a common lexicon and frame of understanding, specifically with regards to civil aviation cybersecurity. In this regard, a general set of principles for the appropriate, global and coordinated management of cybersecurity risks must be further developed at the ICAO level, in close cooperation with Member States and industry. An analysis of the existing framework will be conducted in order to determine the best way to achieve seamless and effective alignment of these principles and models.

5.3 DEVELOPMENT OF COMMON TERMINOLOGY

5.3.1 A common civil aviation cybersecurity-related terminology will be developed under the umbrella of ICAO, taking into account existing cybersecurity-related terminology and aviation-related terminology and frameworks to allow all aviation stakeholders, whatever their background and activity level, to understand each other.

5.3.2 The aim is to facilitate cybersecurity-related activities. It does not mean that a single definition will be determined and/or agreed for all terms. It is acceptable that various definitions exist for the same term (e.g. likelihood, severity, occurrence etc.), provided that they are context-specific and that this repetition does not generate confusion that may cause ineffective management of civil aviation cybersecurity risks. Specifically, with an increased focus on integrated safety and security risk management, ICAO must pay very close attention to ensure terminology is aligned correctly. Recalling the initial context statement above, and the clarification between security in managing unlawful and intentional acts, and safety being concerned with intentional, non-intentional, and random hazards, this needs further refinement with respect to issues of integrated risk management which may span across both security and safety concerns (ICAO Annex 17 and Annex 19 definitions can be used as baselines). Specifically, with the differing focus of safety and security disciplines (with safety being concerned with intentional, non-intentional or random hazards and security concentrated on unlawful and intentional acts), the introduction of integrated risk management spanning across both disciplines requires clarity of scope and purpose of terms used.

5.4 DEVELOPMENT OF A GENERIC MAP OF INFORMATION EXCHANGE/INTERACTIONS IN AVIATION

5.4.1 A common framework for the identification of high-level functional maps describing the exchanges of information between all aviation actors is a necessary prerequisite to ensure understanding of the cyber-risk landscape. A common framework for identifying high-level mappings for information exchanges between all aviation stakeholders is needed to achieve an understanding of the cyber-risk landscape.

5.4.2 This high-level map of information exchange/interactions mapping should be generic enough to encompass all types of aviation-related operations and should be, as much as possible, independent from the implemented physical and/or technical architectures (functional/service approach). For example, the high-level mapping should, as an example, cover digital data flows for air traffic management, airport-related activities, and digital data flows for aircraft in flight/maintenance operations. This high-level map should leverage any existing efforts that have already been commenced by other groups. The purpose would be to allow each stakeholder to complete/adapt/customize their own map in regard to how it is interacting with other stakeholders. Ultimately, each stakeholder should be able to develop or adapt this mapping to their own unique situation. Accordingly, the results of the security risk assessments conducted by each actor using its own methodology and criteria (that have been made comparable based on a common risk assessment framework – see section 5.6) could be exchanged/shared with other stakeholders, to the extent possible. By working together, using comparable security risk assessment frameworks and

using the map of information exchange/interactions, stakeholders will be able to understand how risks can further propagate to or be managed by other risk-sharing partners, and therefore allow for the sharing of information about risks incurred or induced by each stakeholder.

5.5 DEVELOPMENT OF INTER-ORGANIZATION RISK INFORMATION SHARING

5.5.1 There are many standards and guidance documents which address the responsibility that each organization has for its own cybersecurity management, dealing with internal systems, processes, products and data. However, given that cybersecurity risks to civil aviation are shared between multiple stakeholders, there is a need to look beyond individual organizations. To effectively and efficiently achieve shared risk management, sharing of risk information must be emphasised, which is inherent in conditions where systems, processes, products or data are shared, or are passed from one organization to another.

5.5.2 External agreements should be considered with third party vendors to enable the sharing of sensitive cybersecurity information between an organization and the relevant authorities / regulator to facilitate the management of supply chain risks and threats.

5.6 DEFINE CRITERIA FOR RISK ASSESSMENT POSTURES COMPARABILITY

5.6.1 In a context of risks spanning across multiple organizations, it is essential that stakeholders can understand the end-to-end risks and the related risk appetite of the other stakeholders for the management of these risks. In this context, criteria to enable the easy understanding and comparability of cybersecurity risk assessments should be developed.

5.7 DEVELOPMENT OF APPROPRIATE CIVIL-MILITARY COORDINATION

5.7.1 Where possible and consistent with national law, including but not limited to national security and national defence requirements, competent civil aviation and military authorities should establish capabilities and processes to cooperate on matters related to aviation cybersecurity.

5.7.2 Appropriate cybersecurity-related information-sharing and coordination between civil and military aviation stakeholders from an early stage can be highly beneficial to identify potential cyber threats and risks and thus contributes to successful mitigation of cyber risks to the aviation system.

5.7.3 Information-sharing between civil and military aviation stakeholders is also important in the management of cybersecurity-related crises. States may offer support to their national civil aviation and military stakeholders in the organization of an arrangement to, as far as practicable, facilitate information-sharing through appropriate mechanisms.

5.8 PROMOTION OF GLOBAL AND REGIONAL EVENTS FOR CYBERSECURITY IN CIVIL AVIATION

5.8.1 ICAO will support and plan the organization of global and regional events to promote cybersecurity in civil aviation, as appropriate.

Chapter 6

GOVERNANCE

6.1 ESTABLISHING A GOVERNANCE STRUCTURE

6.1.1 ICAO should establish an internal governance structure for aviation cybersecurity that ensures a holistic, cross-cutting and risk-based approach to cybersecurity and cyber resilience across all relevant aviation domains and areas of expertise.

6.1.2 In addition, States should define and implement national governance and accountability structures for civil aviation cybersecurity, ensuring the development and implementation of national and international cybersecurity and cyber resilience requirements as well as defining the roles and responsibilities of each stakeholder on the national level. Such development should also take into account the required coordination between national civil aviation and cybersecurity competent authorities.

6.2 DEVELOPMENT OF MULTI-ANNUAL PLAN(S) FOR CYBERSECURITY

6.2.1 It is recommended that the Cybersecurity Action Plan (CyAP) be properly aligned with the existing Global Aviation Security Plan (GASeP), Global Air Navigation Plan (GANP), and Global Aviation Safety Plan (GASP), and cybersecurity aspects should be included and promoted in these plans where appropriate.

6.2.2 In order to ensure the proper national implementation and application of the Global Plans, States are urged to include nationally coordinated and corresponding cybersecurity-related actions in their national safety and security programmes, and air navigation plans.

6.3 DEVELOPMENT OF GOVERNANCE AND ACCOUNTABILITY

6.3.1 ICAO should develop cybersecurity policy guidance to facilitate harmonization and consistency amongst global, regional and national cybersecurity policies.

6.3.2 Cybersecurity governance should be policy-driven and enforced, and accountability needs to be determined for compliance.

6.3.3 States should take tangible actions to continuously improve the efficiency, quality and consistency of cybersecurity management processes at the national level.

6.3.4 If warranted, Information Security Management Systems (ISMS) can be effective tools in managing cybersecurity and may be implemented at the State or organizational level[3].

---

[3] When developing cybersecurity governance at the national level, States may take inspiration from ISO 27001 to define leadership principles, such as: ensuring that information security management system requirements are integrated into the organization's processes; ensuring that the resources needed are available; and ensuring that the information security management system achieves its intended outcomes.

Chapter 7

EFFECTIVE LEGISLATION AND REGULATORY FRAMEWORK

7.1 REVIEW OF EXISTING INTERNATIONAL AIR LAW INSTRUMENTS AS THEY PERTAIN TO THE CYBERSECURITY FIELD

7.1.1 ICAO will conduct an analysis of the existing international air law instruments to identify existing and potential gaps in relation to cyber risks and propose potential solutions to cover identified gaps, if any, with the purpose of further protecting civil aviation.

7.2 KEEPING ICAO PROVISIONS ALIGNED WITH CYBERSECURITY NEEDS

7.2.1 As cybersecurity in aviation matures, provisions may need to be developed to complement or supplement existing SARPs and PANS. This should be done on a case-by-case basis, noting that adding new SARPs or PANS provisions should be avoided to the maximum extent possible and, where necessary, coordinated amongst all relevant stakeholders.

7.3 RATIFICATION OF THE BEIJING CONVENTION AND PROTOCOL

7.3.1 States are encouraged to ratify the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* (Beijing Convention 2010) and the *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft* (Beijing Protocol 2010).

7.4 STATES TO ENSURE APPROPRIATE LEGISLATION AND REGULATIONS ARE FORMULATED AND APPLIED AT THE NATIONAL LEVEL

7.4.1 States are encouraged to evaluate their existing national legal frameworks in the field of cybersecurity and civil aviation in order to determine existing gaps, as well as to ensure appropriate legislation and regulations are in place for specific civil aviation cybersecurity elements. Another key component is the enforcement mechanism that States are encouraged to implement, if it does not already exist in their national legal frameworks, for the criminalization and prosecution of unlawful acts against civil aviation committed using cyber means.

Chapter 8

CYBERSECURITY POLICY

8.1 ELABORATE AND IMPLEMENT CYBERSECURITY POLICIES

8.1.1 A cybersecurity policy needs to be developed at national and organizational levels. States should have in place a clear and actionable cybersecurity policy that includes:

- objectives stemming from results of the civil aviation cybersecurity risks assessments;
- a commitment to satisfy applicable requirements and the way to assess compliance;
- considerations related to the management of and coordination with external dependent parties (ref. to international collaboration chapter);
- a commitment to continuous improvement of the cybersecurity framework;
- provisions to ensure that the policy is fully documented and is available as official information; and
- provisions to ensure that the policy is properly disseminated.

8.2 IDENTIFY AND EVALUATE CYBER-RISKS TO CIVIL AVIATION

8.2.1 One of the challenges of risk identification and evaluation activities is to be able to anticipate the rapid changes of the origins and characteristics of threats. Anticipation of changing threats is key to help the air transport system proactively adapt its protection strategy not only according to current threats, but also in light of potential future threats. Thanks to this anticipation, the civil aviation sector should be able to be more proactive in a context whereas there is asymmetry between agility of the attackers that are very agile and adaptive and the defenders that, given the complexity of the system to be protected, are slow to react. In this scenario, this proactive approach becomes even more critical. Hence, it is necessary to develop a cybersecurity risk identification and evaluation framework supporting this need, to help mitigate these risks.

8.2.2 It is recommended that cybersecurity risks be identified and assessed taking into account all the potential consequences of an attack on the civil aviation system (security, safety, efficiency, resilience, continuity of service, etc.), as well as all potential sources of threat and the vulnerabilities that exist to such threats. This activity should build on the cyber-risk matrices previously developed under the auspices of the Aviation Security Panel Working Group on Threat and Risk (WGTR).

8.2.3 Since a significant proportion of cybersecurity risks for civil aviation are shared by many stakeholders, it is recommended to consider the mapping of information exchanges/interactions in aviation (see Chapter 5.1). This mapping should be used as a means of guaranteeing the exhaustiveness of the scenarios considered and to enable stakeholders to understand how they interact with each other and their dependencies on risks.

8.2.4 As the level of severity of cybersecurity risks will vary over time and these risks can evolve rapidly compared to others, it is recommended to consider a means to adapt any global aviation response to these risks that can be deployed in a rapid and coherent manner (e.g. balancing the need for aviation standards, guidance materials, non-aviation best practices, and using/relying on other domain responses).

8.2.5 It is recommended that the identification and evaluation of cybersecurity risks be entirely carried out and coordinated by a group of experts composed of civil aviation cybersecurity experts, or, failing that, by a team of cyber and civil aviation experts, preferably with an extensive background in cybersecurity.

8.2.6 This group of experts should be responsible for the development of a Global Cybersecurity Risk Context Statement.

Chapter 9

INFORMATION SHARING

Sharing of cybersecurity-related information is essential to the managing cybersecurity risks to civil aviation systems. In recognition that promoting information sharing is a key element of building cybersecurity culture, civil aviation stakeholders should develop or leverage existing, and implement, programmes enabling the sharing of information within their organizations and with external parties, to the extent possible. Through these programmes, they should develop partnerships and share substantive information with other stakeholders which own and operate civil aviation infrastructure, and develop information-sharing schemes and practices within their organizations.

These information-sharing programmes should enable the development, operation and adjustment of civil aviation cyber defences against known and emerging cyber threats. They should help develop:

- Situational awareness in both normal day-to-day operations, and during a crisis, incident, or event;
- Operational and tactical risk management in anticipation of, and in response to, a threat;
- Strategic planning to build capabilities that strengthen cyber-security and resilience for the future.

9.1 DEVELOPMENT OF RISK INFORMATION SHARING

9.1.1 Sharing cyber-related information has bilateral and multilateral dimensions – any combination amongst and across (nationally, regionally, globally) the following parties:

- national cyber authorities;
- national civil aviation authorities;
- national military aviation authorities;
- other aviation stakeholders (operators, service providers and manufacturers); and
- non-aviation stakeholders (IT and communications providers and supply chain).

9.1.2 It is recognized that there are many types of cybersecurity-related information, such as:

- *Cyber-intelligence*, such as threat landscape, intelligence about cyber threat actors' capability, and intent.
- *Indicators of Compromise (IoCs)*.
- *Tactics, Techniques and Procedures (TTPs)*, such as scenarios of attacks and preferred methods used by hackers.
- *Vulnerabilities*, such as in hardware, software, service, protocol, standard, etc., including potential exploit scenarios.
- *Incident reports.*

9.1.3 Depending on national legislation and the nature of the cyber-related information, there could be various methods and constraints to share the information with various recipients (e.g. national cyber authority, national civil aviation authority, national military aviation authority, and other aviation stakeholders).

9.1.4 Information-sharing, collaboration needs (including but not limited to times of crisis), and policies should be identified at the global, regional and national levels.

9.1.5 It is recommended to use the Traffic Light Protocol (TLP)[4] to state the level of distribution/restrictions when distributing and further sharing cyber-related information.

9.1.6 To the extent possible, cyber-related information, which may contain some sensitive information, should be de-identified or sanitized before sharing, rather than not sharing it at all.

9.2 DEVELOPMENT OF PRINCIPLES AND GUIDANCE FOR SECURITY RESEARCHER RESPONSIBLE DISCLOSURE

9.2.1 Given the growing interest of the security researchers' community in civil aviation cybersecurity, and to avoid irresponsible disclosure of potential findings that may be detrimental to the safety, security, efficiency, or continuity of civil aviation, principles for the responsible disclosure of vulnerabilities discovered by security researchers, or third parties, need to be defined to ensure that disclosures are not detrimental to civil aviation cybersecurity. This should take into consideration recommendation 4.4 of the Cybersecurity Strategy.

9.2.2 Guidance for these principles (addressing, amongst other concerns, e.g. discovery, manufacturer notification, investigation, resolution, industry notification, resolution, and lastly, public release) should be established between, on one hand, researchers and third parties, and on the other hand, aviation authorities and aviation stakeholders to ensure, to the maximum extent possible, that such vulnerability research/discovery and disclosure activities have no impact on safety and service provision. Ideally guidance would not only address responsible disclosure processes, but also include awareness and educational elements.

9.3 DEVELOPMENT OF A GLOBAL NETWORK OF REGIONAL/NATIONAL CYBER AUTHORITIES FOR CIVIL AVIATION PURPOSES

9.3.1 Cybersecurity responsibility within States and industry is not uniformly assigned, and appropriate expertise is spread across a wide range of aviation and non-aviation stakeholders and functional areas. The innate concern of this variety creates difficulty in identifying the appropriate point of contact within an entity, and establishment and maintenance of formalized communication channels between stakeholders. Guidance on establishing and maintaining a single point of contact for civil aviation cybersecurity-related matters within States and organizations can facilitate the building of global, regional and national communication channels, build appropriate cybersecurity communities, and drive cybersecurity culture.

9.4 GLOBAL CYBERSECURITY INFORMATION SHARING CAPABILITY FOR AVIATION

9.4.1 Civil aviation information-sharing capabilities may be developed transversely at the global, regional, and/or national levels to foster the exchange of cybersecurity-related information.

9.4.2 Information sharing forums may include public-public, public-private, and private-private structures. Stakeholders should engage in trusted communities to facilitate exchange of both best practices and threat intelligence.

---

[4] Refer to ICAO guidance material on "Guidance on Traffic Light Protocol"

Chapter 10

INCIDENT MANAGEMENT AND EMERGENCY PLANNING

10.1 DEVELOPMENT OF INCIDENT RESPONSE CAPABILITIES AND EMERGENCY RESPONSE PLANNING

10.1.1 All stakeholders are strongly encouraged to develop and test incident response and emergency plans in a coordinated manner with their operational partners, which includes:

- making use of existing contingency plans that are already developed and/or amending these plans to include provisions for cybersecurity;
- civil aviation stakeholders developing and maintaining appropriate scalability that provides for the safety, security and continuity of air transport operations during possible cyber incidents;
- development of provisions for cybersecurity incident response and recovery capabilities, including contingency and emergency response plans;
- involving military aviation stakeholders in the planning process, to proactively establish lines of communication;
- achieving acceptable performance levels and satisfying the requirements to maintain minimum service levels of essential services;
- developing harmonized categorization for cyber incident reporting, and coordinating civil aviation cybersecurity incident reporting schemes at the national, regional, and, where applicable, international levels; and
- aviation stakeholders should periodically conduct live exercises to test the validity of assumptions made in planning and table top exercises.

10.2 INCIDENT DETECTION, ANALYSIS AND RESPONSE MEANS AT THE STAKEHOLDER LEVEL

10.2.1 To the extent possible, incident response plans should be implemented, and stakeholders should develop the capabilities for cybersecurity incident detection, analysis and response at all levels. It is important to monitor the cybersecurity status of those systems/services as deemed critical in supporting civil aviation, in order to detect potential problems and to track the ongoing effectiveness of protective security measures. Once detected, cybersecurity incidents should be analysed and appropriate response plans put into action; these should include mitigating actions to limit the impact of the cybersecurity incident.

10.3 DEVELOPMENT OF A CRISIS COORDINATION CELL FOR CIVIL AVIATION CYBERSECURITY

10.3.1 A civil aviation crisis coordination cell embedding civil aviation cybersecurity expertise should be implemented when possible (building on already existing mechanisms) and, where appropriate, military aviation stakeholders should be involved.

10.3.2 Periodic exercises should be conducted regularly, in particular table top exercises (TTX), with industry participation from all relevant stakeholders where appropriate.

Chapter 11

CAPACITY BUILDING, TRAINING AND CYBERSECURITY CULTURE AND EDUCATION

11.1 DEVELOPMENT OF TECHNICAL CAPACITY, TRAINING AND CYBERSECURITY CULTURE AND EDUCATIONAL MATERIAL

11.1.1 Education, training and awareness on civil aviation cybersecurity should be defined and promoted at the global, regional, and national levels.

11.1.2 Cybersecurity culture and educational activities should be promoted from the senior management level throughout civil aviation organizations, and should highlight the key roles of and expectations from the different actors. It should lead to the development of a cross aviation safety and aviation security cybersecurity body of knowledge, and should include:

- notions of secure-by-design principles to mitigate cyber threats, in coordination with the safety community. These notions should help the aviation safety community make better-informed decisions when addressing cyber threats;
- a coordinated approach between security and safety stakeholders, recognizing that security controls must not have a negative impact on safety of flight, enabling the transfer of technical knowledge, and ensuring that informed decisions are taken on the basis of a mutually understood risk landscape;
- notions of cyber hygiene practices for operational and support staff that should help prevent potential adverse impacts to the civil aviation system caused by the increasing number of "Commercial Off the Shelf" (COTS) products and non-specific malware; and
- notions of "Just Culture" from the safety community to enable and stimulate self-reporting of occurrences that results from unintended behaviour by personnel (e.g. unintentional malpractice in handling an USB Stick).

11.1.3 In carrying out these activities, emphasis should be placed on impact or potential impact.

11.1.4 The development of this cybersecurity culture and promotion of cybersecurity culture and educational material should help develop a mutual/common understanding in the safety and security communities of the cybersecurity risk landscape, as well as a mutual confidence in the countermeasures being put in place.

11.1.5 ICAO should encourage trans-national/trans-regional exchange programmes on cybersecurity education and training.[5]

11.1.6 Cybersecurity culture and education activities should not only focus on systems' operation but rather on their entire system life-cycle, including:

[5] As for example initiatives for multinational campus or EU Cybersecurity Competence network and centres

- requirement (security an integrated part already in the requirement phase);
- design (follow a secure-by-design strategy, security for hardware, software and data, change management, vulnerability management);
- development (secure environment, continuous and integrated security testing);
- manufacturing/acquisition (including information and operational technologies' hardware and software supply chain);
- operation (including access management, data integrity, secure systems operation);
- maintenance (including patching and update strategy); and
- disposal (including management of credentials and residual data on storage devices).

Chapter 12

CONCLUSION

The Cybersecurity Action Plan brings together ICAO, States, industry, and other stakeholders in a holistic and coordinated effort to address current and emerging cybersecurity challenges. It highlights that cybersecurity is a cross-cutting issue that involves all domains of the aviation sector. The plan assists in implementing the ICAO Aviation Cybersecurity Strategy and moving towards creating a robust global cybersecurity framework.

— — — — — — — —

APPENDIX A

Cybersecurity Action Plan Roadmap

CYBERSECURITY STRATEGY GENERAL ACTIONS

Priority Outcome	**DEVELOP A GLOBAL AND AGREED VISION**
Priority Actions	• Recognize that it is imperative to develop a comprehensive and agreed cybersecurity vision as a foundation to solid and coordinated global aviation cybersecurity risk management. • Recognize that the civil aviation sector shall be resilient to cyber-attacks and remain safe and trusted globally, whilst continuing to innovate and grow. • Recognize that civil aviation cybersecurity risks are to be treated under the Convention on International Civil Aviation.

Actions

Action #	By	Specific Measures/Tasks	Indicators	Priority	Start Date of Implementation
CyAP 0.1	ICAO, Member States, and Industry	ICAO to develop a model Cybersecurity Policy for reference by Member States and Industry when developing their own national/organizational policies.	The model is available to Member States and Industry.	High	2021
CyAP 0.2	ICAO and Member States	Commence the implementation work of the ICAO Aviation Cybersecurity Strategy at national level (as instructed in Resolution A40-10) (in order to verify how States implement the Strategy, a set of metrics need to be developed to measure the implementation of certain actions).	National evidence of commencement of implementation work.	High	2023
CyAP 0.3	ICAO	Conduct surveys to establish how States have implemented the ICAO Aviation Cybersecurity Strategy. (survey to ask if States have developed an action plan to implement the Strategy).	ICAO survey/questionnaire sent to the Member States.	High	2021-2022

CYBERSECURITY STRATEGY PILLARS

Priority Outcome	**1. ACHIEVE INTERNATIONAL COOPERATION**
Priority Actions	• Develop cooperation at the national, regional, and international levels between all stakeholders. • Recognize mutually the efforts (develop, maintain and improve cybersecurity) to protect civil aviation. • Pursue regulatory harmonization at the international, regional and national levels in order to promote global coherence and ensure interoperability of protection measures. • Engage States in addressing cybersecurity in international civil aviation. • Facilitate and promote international events in the cybersecurity field. • Recognize that cybersecurity is a shared responsibility across all segments in the global civil aviation system.

Actions

Action #	By	Traceability to the Aviation Cybersecurity Strategy	Traceability to Chapter 5	Specific Measures/Tasks	Indicators	Priority	Start Date of Implementation
CyAP 1.1	ICAO and Member States	1.1	5.2	Include Cybersecurity in ICAO safety and security oversight programmes – include relevant Standards in the ICAO audit programmes (such as USOAP and USAP).	ICAO audit programmes from both safety and security perspectives include cybersecurity-relevant Standards.	High	Ongoing
CyAP 1.2	ICAO	1.1	5.1 See also CyAP 4.6 (Para 8.2 Action Plan)	Conduct surveys of cybersecurity initiatives/practices to establish how States and industry are managing civil aviation cybersecurity.	Results of questionnaires, number of initiatives and regions.	High	Ongoing
CyAP 1.3	ICAO	1.1	5.1	Develop an inventory of all the cyber-security initiatives engaged in the different ICAO groups of experts.	An ICAO Aviation Cybersecurity Work Programme is developed and maintained by the Ad Hoc Cybersecurity Coordination Committee.	High	2024

CyAP 1.4	ICAO and Member States	1.2	5.2.3 and 5.5 See also CyAP 5.1 (Para 9.2 Action Plan)	A) Develop models of Memoranda of Understanding/Collaboration, External Agreements. B) Provide guidelines on how to develop these agreements.	Availability of template and guidelines.	Low	2023-2024
CyAP 1.5	ICAO, Member States, and Industry	1.2	5.3	Develop a consistent and agreed civil aviation cybersecurity related terminology to allow all aviation stakeholders, whatever their background and activity level, to understand each other with regards to cybersecurity.	Publication of a cybersecurity glossary.	Medium	2023
CyAP 1.6	ICAO, Member States, and Industry	1.2	5.4	ICAO to develop, a common framework for the identification of high-level functional map describing the exchanges of information between aviation actors (e.g., ANSP, AOC, A/C, Airport, MET, MRO, CNS), as a necessary condition to facilitate understanding of the cyber-risk landscape. Member States and Industry to develop such frameworks at national and organizational levels.	Existence of common framework and identified generic map of information exchanges/interactions in aviation. Awareness and understanding of the functional map.	High	2024
CyAP 1.7	ICAO and Member States	1.2	5.7 See also CyAp 6.2 and Para 10.2 of the Action Plan)	ICAO to establish models of cooperation between civil and military aviation in order to develop, where appropriate, models/guidance for civil and military interoperable aviation interfaces. Determine criteria and level of appropriate interaction.	Availability of models/guidance for civil/military cyber cooperation and interoperability. List of criteria and minimal required interactions published.	High	2023
CyAP 1.8	ICAO, Member States and Industry	1.3	5.8	Plan, organize and support international and regional events to promote cybersecurity in civil aviation.	Events, Awareness building, international cooperation.	N/A	Ongoing

CyAP 1.9	ICAO, Member States, and Industry	1.3	5.4	Ensure that all relevant stakeholders are engaged in discussions and activities regarding cybersecurity in civil aviation. Continuous involvement and outreach with relevant stakeholders.	Publish results of common efforts. Publish proof of engagement, such as partnerships, group membership, etc.	High	Ongoing
CyAP 1.10	ICAO, Member States, and Industry	1.2	5.2.2	Develop an international aviation trust framework that allow entities to interoperate according to the trust they have in other stakeholders.	Establishment of a trust framework used by many organizations.	High	2024-2025

Priority Outcome	**2. DEVELOP GOVERNANCE AND ACCOUNTABILITY**
Priority Actions	• Encourage, support and build upon the ICAO Cybersecurity Strategy. • Develop clear national governance and accountability for civil aviation cybersecurity. • Ensure coordination at the State level between Civil Aviation authorities and the competent national authorities for cybersecurity. • Establish appropriate coordination channels among various State authorities and industry. • Include cybersecurity in national civil aviation safety and security programmes. • Include cybersecurity in global and regional plans. • Work towards a common baseline for cybersecurity Standards and Recommended Practices.

Actions

Action #	By	Traceability to the Cybersecurity Strategy	Traceability to Chapter 6	Specific Measures/Tasks	Indicators	Priority	Start Date of Implementation
CyAP 2.1	ICAO and Member States		6.1	Establish a governance structure in the civil aviation cybersecurity field.	Identification of adequate governance structure(s) for civil aviation cybersecurity.	N/A	2021-2023
CyAP 2.2	ICAO and Member States	2.2	6.3	ICAO to develop a general set of principles on adequate management system(s) for civil aviation cybersecurity. Member States to develop	Publication of general principles.	High	2023-2024

				such principles at national level following the ICAO model.			
CyAP 2.3	ICAO, Member States, and Industry	2.2	6.3.2 See also para 8.1. of the Action Plan	Develop guidance material to support organizations in implementing coordinated cybersecurity management frameworks to support the establishment of a systematic approach to manage aviation cybersecurity risks and assess those frameworks' maturity and effectiveness.	Publication of guidelines.	High	2023
CyAP 2.4	ICAO and Member States	2.2	6.3	Promote coordination mechanisms between civil aviation authorities and cybersecurity authorities.	ICAO Survey – number of identified existing coordination mechanisms in place.	Medium	2022
CyAP 2.5	ICAO	2.3	6.2.1 See also CyAP 1.9 (Para 5.2 Action Plan)	ICAO to include cybersecurity in regional and global plans to ensure the safety, security, and resilience of aviation.	Updated Plans published.	N/A	2022-2023
CyAP 2.6	ICAO		6.2	ICAO to prepare best practices registry/guidelines section in the repository.	ICAO Repository of best practices.	N/A	2020-2021
CyAP 2.7	ICAO, Member States and Industry	3.2	6.3	ICAO to develop model procedures to report cyber incidents, including incident classification guidance. Member States and Industry to develop national and organizational procedures to report cyber incidents in a timely and effective manner.	Cyber incidents reporting procedures / number of reported incidents according to the procedures.	High	2022-2023
CyAP 2.8	ICAO and Member States	2.2	6.2	ICAO to evaluate the extent to which Member States include cybersecurity in their national civil aviation safety and security programmes, and air navigation plans.	ICAO Survey - Number of States that have included cybersecurity in their national civil aviation safety and security programmes.	High	Survey 2022, Further actions ongoing

Priority Outcome	3. DEVELOP EFFECTIVE LEGISLATION AND REGULATIONS
Priority Actions	• Ensure that international legal instruments provide an appropriate framework for the deterrence of cyber incidents as well as the prosecution of their perpetrators. • Analyze existing national legislation and update or adopt national legislation as necessary to allow for the deterrence, investigation, and prosecution of cyber-attacks that impact the safety, security, efficiency, or continuity of civil aviation. • Ensure that appropriate national regulations and legislation are in place for civil aviation cybersecurity. • Develop appropriate guidelines for States and industry in implementing cybersecurity-related provisions.

Actions

Action #	By	Traceability to the Cybersecurity Strategy	Traceability to Chapter 7	Specific Measures/Tasks	Indicators	Priority	Start Date of Implementation
CyAP 3.1	Member States	3.3	7.4	Member States to ratify Beijing instruments.	Number of States having ratified the Beijing instruments.	High	Ongoing
CyAP 3.2	ICAO	3.3	7.3	Analysis of international air law instruments.	Review and Gap Analysis of Relevant International air law instruments.	High	2022
CyAP 3.3	ICAO and Member States	3.3 and 3.4	7.2	Analysis of existing national legislation in the civil aviation cybersecurity field and identify gaps, including in criminal law.	Survey on status of national legislation with regards to addressing unlawful acts against civil aviation committed through cyber means.	Medium	2023-2024
CyAP 3.4	ICAO	3.3	7.1	Review existing ICAO Standards and Recommended Practices to identify need for potential cybersecurity updates.	Review and Gap Analysis of ICAO SARPs.	High	2022
CyAP 3.5	ICAO	3.2		Create, review and amend guidance material related to implementing civil aviation cybersecurity requirements.	Publication of civil aviation cybersecurity guidance material.	High	2021 and ongoing

Priority Outcome	4. DEVELOP A CYBERSECURITY POLICY
Priority Actions	• Ensure that cybersecurity is part of civil aviation safety and security systems and comprehensive risk management frameworks. • Ensure varying civil aviation cybersecurity risk assessment methodologies retain comparability. • Develop cybersecurity policies considering the complete life cycle of aviation systems.

Actions

Action #	By	Traceability to the Cybersecurity Strategy	Traceability to Chapter 8	Specific Measures/Tasks	Indicators	Priority	Start Date of Implementation
CyAP 4.1	Member States and Industry	4.1	8.1	Member States and Industry to ensure commitment of their management to addressing civil aviation cybersecurity and cyber resilience.	Awareness campaign / Proof of commitment, such as declarations of commitment, defined responsibilities in the cybersecurity field in the management manuals of authorities and organizations.	Medium	2022-2023
CyAP 4.2	ICAO, Member States, and Industry	4.3	8.2 See also para 5.11 Action Plan	Encourage cybersecurity Research & Development in civil aviation by engaging with universities, institutes, researcher communities etc.	Number of interactions and projects.	High	2022-2023
CyAP 4.3	Member States, and Industry	4.2	5.6 and 8.2	Define criteria for a shared trans-organizational risk assessment along with the information to be shared and the needed criteria for risk comparability. Member States to define such criteria at national level, and the Industry at organizational level.	Publication of objectives and criteria for a shared trans-organizational risk assessment.	High	2023
CyAP 4.4	ICAO, Member States, and Industry	4.3	8.1	Develop a policy for security by design as a basis for a secure life-cycle of civil aviation systems.	Policy for secure life-cycle of civil aviation systems formulated.	Medium	2022-2023

CyAP 4.5	ICAO, Member States, and Industry	4.2	8.2	ICAO to develop international forums to discuss trans-organizational/trans-functional cybersecurity and cyber resilience targets and minimum level of functionalities essential to the civil aviation sector. Member States to develop such forums at national and regional levels, and Industry to develop specific forums and be actively involved in the forums established by ICAO and Member States.	Number of fora to discuss targets.	High	2022-2023
CyAP 4.6	ICAO, Member States, and Industry	4.3	8.2	Establish an inventory of existing civil aviation cybersecurity risk management initiatives (risk profiles, scenarios, vulnerability management, and risk assessments).	Availability of a cybersecurity risk management initiatives' repository.	Medium	2023-2024
CyAP 4.7	ICAO, Member States, and Industry	4.3	8.3	ICAO to develop a list of strategic cyber risk scenarios at international level. Member States and Industry to contribute and develop similar lists at national and organizational levels.	Availability of 10 cyber risk scenarios.	High	2023-2024
CyAP 4.8	ICAO, Member States, and Industry		8.2	ICAO to develop risk profiles for each operational domain. Member States and Industry to contribute by developing similar risk profiles at national and organizational levels.	Availability of risk profiles.	High	2023
CyAP 4.9	ICAO		8.2	Develop a Global Cybersecurity Risk Context Statement.	Publication of Global Cybersecurity Risk Context Statement.	High	2023

Priority Outcome	5. DEVELOP INFORMATION SHARING CAPABILITIES
Priority Actions	• Develop or leverage existing sharing of information platforms and mechanisms which are recognized, in line with existing ICAO provisions, to enable cyber situational awareness thus allowing prevention, early detection and mitigation of relevant cybersecurity events. • Ensure that any cyber incident or vulnerability which may represent a significant risk to aviation safety and/or security is reported to the competent authority.

Actions

Action #	By	Traceability to the Cybersecurity Strategy	Traceability to Chapter 9	Specific Measures/Tasks	Indicators	Priority	Start Date of Implementation
CyAP 5.1	ICAO	5.1	9.1 & 9.2	ICAO to develop guidance for information sharing.	Guidance document for information sharing available to the community.	High	2022-2023
CyAP 5.2	ICAO	5.1	9.1	ICAO, with support of the Member States and Industry, to identify cybersecurity-related information sharing, collaboration needs (including but not limited to times of crisis), and policies.	Develop a list of potential information to be shared.	Medium	2022-2024
CyAP 5.3	ICAO	5.1	9.1	Develop guidance on the use of TLP (Traffic Light Protocol) to state the level of distribution/restrictions when distributing and further sharing cyber-information.	Publish policy Guidance for the use of TLP when distributing and sharing cyber information.	High	2021
CyAP 5.4	ICAO, Member States, and Industry	5.2	9.2	Consider the feasibility of defining criteria for the responsible disclosure of cybersecurity vulnerabilities.	Availability and publication of principles for the responsible disclosure of vulnerabilities if deemed feasible.	High	2023
CyAP 5.5	ICAO and Member States	5.2	9.4	ICAO to develop and maintain a point of contact network at international level for civil aviation cybersecurity-related matters for Member States and Industry. Member States to cooperate with ICAO by developing such network points of contact at national levels.	Establishment of a civil aviation cybersecurity point of contact network. Publish the network point of contact for each Member State.	Medium	2024-2025

Priority Outcome	6. DEVELOP INCIDENT MANAGEMENT AND EMERGENCY PLANNING
Priority Actions	• Ensure appropriate and scalable plans that provide for the continuity of safe and secure civil aviation operations in case of cyber incidents. • Ensure leveraging existing contingency plans to include provisions to respond to, and recover from, cybersecurity incidents, and regularly/periodically conduct exercises to test the capabilities to detect, respond and recover from cyber incidents.

Actions

Action #	By	Traceability to the Cybersecurity Strategy	Traceability to Chapter 10	Specific Measures/Tasks	Indicators	Priority	Start Date of Implementation
CyAP 6.1	Member States and Industry	6.1	10.1	Member States to establish targets and minimum levels of functionalities essential to the civil aviation sector. Industry to apply the targets developed.	Publish a list of targets and minimum acceptable levels of functionalities for aviation continuity.	High	2022-2023
CyAP 6.2	ICAO and Member States	6.1	10.2	ICAO to develop guidance and processes to include military stakeholders in cybersecurity incident response planning for civil aviation. Member States to develop procedures and cooperation agreements between civil and military aviation authorities.	Development and publication of guidance regarding civil-military cooperation processes and procedures in civil aviation cybersecurity incident response.	High	2022-2023
CyAP 6.3	ICAO, Member States, and Industry	6.1.	10.1	ICAO to develop guidance for civil aviation cyber-incident response and recovery capabilities, including contingency and emergency response plans. Member States and Industry, following the ICAO guidance, to develop such guidance at national and organizational levels.	Publish guidance for civil aviation cyber-incident response and recovery capabilities, including contingency and emergency response plans.	High	2022-2023
CyAP 6.4	Member States	6.1.	10.2 and 10.3	Member States to develop and implement capabilities and plans for civil aviation cybersecurity incident detection, analysis and response at operational level.	Survey to track the level of implementation.	High	2023-2024

CyAP 6.5	ICAO and Member States	6.1.	10.1	Develop processes for civil aviation cybersecurity crisis coordination, including at national and international levels.	Definition of cybersecurity crisis coordination processes established. Publication of guidance material.	Medium	2024-2025
CyAP6.6	Member States and Industry	6.1	10.3	Conduct periodically table top and live exercises.	Sharing of lessons learned, as appropriate.	High	2022-2023

Priority Outcome	**7. DEVELOP CAPACITY BUILDING, TRAINING AND CYBERSECURITY CULTURE**
Priority Actions	• Ensure appropriate role-based qualifications of personnel in both aviation and cybersecurity. • Increase awareness of cybersecurity, including activities to establish appropriate cyber hygiene. • Ensure proper curricula on aviation cybersecurity are included in the national educational framework, in order to ensure the development of a cross aviation safety and security body of knowledge throughout the organization, including its senior management. • Foster cybersecurity innovation and appropriate research and development. • Include cybersecurity in the ICAO Next Generation of Aviation Professionals' strategy.

Actions

Action #	**By**	**Traceability to the Cybersecurity Strategy**	**Traceability to Chapter 11**	**Specific Measures/Tasks**	**Indicators**	**Priority**	**Start Date of Implementation**
CyAP 7.1	ICAO, Member States, and Industry	7.1.	11.1	Define and promote a civil aviation cybersecurity culture and education.	Availability of courses and guidance material related to civil aviation cybersecurity culture.	Medium	2022-2023
CyAP 7.2	Member States, and Industry	7.2.	11.1	Member States and Industry to develop appropriate role-based aviation cybersecurity training requirements at all levels within their organizations.	Develop appropriate role-based aviation and cybersecurity training.	High	2022-2023
CyAP 7.3	ICAO and Member States	7.3.	11.1	ICAO to include cybersecurity in the Next Generation of Aviation Professionals strategy.	Cybersecurity included in NGAP strategies.	Medium	2022-2023

				Member States to include cybersecurity in their national strategies related to the NGAP strategy.			
CyAP 7.4	ICAO	7.3.	11.1	ICAO to analyse means and ways to support cybersecurity role-based competency requirements.	Cybersecurity role-based training included in ICAO Doc 7192 and 9868 if deemed feasible.	High	2023-2025
CyAP 7.5	ICAO, Member States, and Industry	7.3.	11.1	Development of capacity building activities.	Availability of aviation cybersecurity training courses.	High	Ongoing

— END —