SOUTH AFRICAN CIVIL AVIATION AUTHORITY

TECHNICAL GUIDANCE MATERIAL for the Development of Aviation Cybersecurity Programme

SUBJECT: TECHNICAL GUIDANCE MATERIAL FOR THE DEVELOPMENTS OF AVIATION CYBERSECURITY PROGRAMME

EFFECTIVE DATE: 28 March 2022

APPLICABILITY:

This TGM is applicable to Aviation security entities, who are required to safeguard aviation infrastructure systems and communication data against unlawful interference as stipulated in the NASP.

PURPOSE:

The TGM is intended to guide and assist aviation community in developing a proportionate and effective cyber security programme that enables the management of cyber security risks without compromising aviation safety, security or information and system management through maintaining the:

a. Confidentiality: the assurance that aviation data is not disclosed to unauthorised persons, processes, or devices. It includes both the protection of operational aviation information and the protection of password and configuration information.
b. Integrity: assures that aviation data is not modified by unauthorised entities or through unauthorised processes. Integrity supports the assurance that aviation data is not accidentally or maliciously manipulated, altered, or corrupted. Integrity also means that detection occurs with no or minimal false alarms when data has been modified; and that the source of this modification must be identifiable.
c. Availability: assures timely, reliable, continued access to aviation data by authorised users. Availability controls protect against degraded capabilities and denial of service conditions.
d. Authentication: assurance of the identity of message senders and receivers. Authentication supports the validation of messages and information system requests.
e. Authorisation: the verifiable identity of each entity handling any asset must be checked to confirm it possesses appropriate permission and privilege.
f. Non-repudiation: assurance that the data sender is provided with proof of delivery, and the recipient is provided with proof of the sender's identity. This provides assurance that sender and receiver receive confirmation of the transmission and receipt of the data.
g. Traceability: All actions performed on each asset must be logged in a format and for a time period that can satisfy both regulatory and consumer needs

REQUIREMENTS

Additional relevant resources for information can be found in the following materials based on the distinctiveness of what cybersecurity involves within the organisational aviation ecosystem:

1. REFERENCE:

i. ICAO Annex 17 (section 4.9)
ii. ICAO Aviation Security Risk Context Statement
iii. ICAO Aviation Security Manual -DOC 8379
iv. ICAO Aviation cybersecurity strategy and Action Plan
v. ICAO Air traffic Management security Manual -Doc 9985
vi. National Aviation Security Programme (NASP)
vii. SA-CATS-AVSEC Parts
viii. NIST Cybersecurity Framework
ix. ISO 27000
x. NIST Risk Management Framework

2. TERMS AND ABBREVIATIONS:

TERM	DEFINITION
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 organisation's risk acceptance level designated to treat and manage risks. Source ISO/IEC27000:2009
Cybersecurity	refers to the body of technologies, controls and measure, and process and practices designed to ensure confidentiality, integrity, availability and overall protection of systems, networks, programmes, devise, information and data from attack, damage, unauthorised access, use and /or exploitation.
Cybersecurity culture	refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms, and values of people regarding cybersecurity and how they manifest in people's behavior with information technologies-ENISA
Cybersecurity policy	A document with the intention and direction of an organisation, for the management of cybersecurity threats, as expressed by top management. It is a written document in an organisation an outlining how to protect the organisation from cybersecurity threats, and how to handle incident and event when they do occur.
Events	Identified occurrences in a system, service or network state indicating a possible breach of information security policy or failure of control, or a previously unknown situation that may be security relevant and shall not be understood as (safety) occurrence terms that only embraces the events which have or could have significance in the context of aviation safety
Incident	Singler or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information secuirty. Source ISO/IEC 27035-1
Information security	Preservation of confidentiality, integrity, and availability of information. In addition, other properties such a s authenticity, accountability, non-repudiation and reliability can be involved. Source ISO/IEC 27000:2018
Information sharing	The process through which information is provided by one entity to one or more other entities to facilitated risk -based decision making and promote best practices

ABBREVIATION	DESCRIPTION
caISMS	Civil aviation Information Security Management System
CIA	Confidentiality, Integrity and Availability
CSIAD	Critical system, Information, Assets and Data
GRC	Governance, risk and Compliance
ISO	International Standards operator
NIST	National International
TLP	Traffic Light Protocol
RS	Risk Specialist
E: AVSEC	Executive: Aviation Security

3. GENERAL

3.1. In accordance with the provisions contained in Annex17– Security, and measures concerning cyber threats
Standard 4.9.1 stipulate that: "Each Contracting State shall ensure that operators or entities as defined in the National Civil Aviation Security Programme or other relevant national documentation identify their critical information and communications technology systems and data used for civil aviation purposes and, in accordance with a risk assessment, develop and implement, as appropriate, measures to protect them from unlawful interference".

3.2. Furthermore, the DOC 8973 chapter 18 outline a framework for safeguarding and provide approach regarding:

3.2.1 Identification of threats and risks from possible cyber incidents and attack to civil aviation operations; critical systems and data, and the serious consequences that can arise

3.2.2 Defining the role and responsibilities of the entire aviation industry operator towards cybersecurity.

3.3. The development of a common understanding among operators on cyber threats and risks, and to establish a common criterion to determine the criticality of the assets and systems that need to be protected.

3.4. To encourage government/industry coordination pertaining to aviation cybersecurity strategies, policies, and plans, as well as sharing of information to help identify critical vulnerabilities that need to be addressed.

3.5. Develop and participate in government/industry partnerships for the systematic sharing of information on cyber threats, incidents, trends, and mitigation efforts.

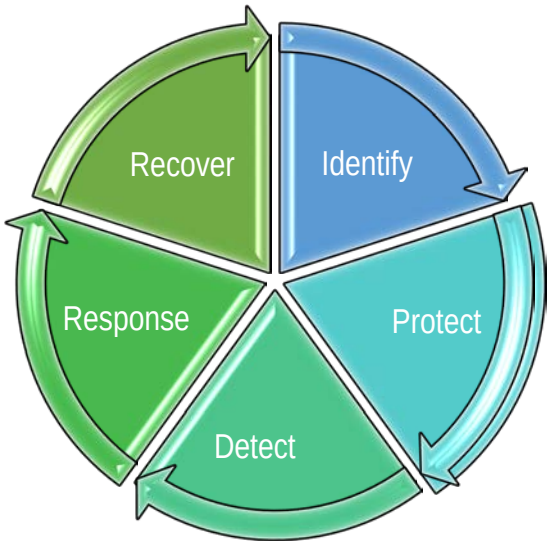
3.6. Based on a common understanding of cyber threats and risks, to adopt a flexible risk-based approach for the protection of critical aviation systems through the implementation of cybersecurity management systems.

3.7. Encourage a robust all-around cybersecurity culture within national agencies and across the aviation sector,

3.8. Establish policies and allocate resources when needed to ensure that, critical aviation systems are resilient and secure to ensuring integrity and confidentiality of data.

3.9. Based on the ICAO cybersecurity provision and the national information and cybersecurity approach, to consult the NIST framework and ISO 27000 suite as recommended best practices to inform the protection methods.

4. THE TGM IS DEFINED THROUGH THE APPLICATION OF THE FIVE (5) PILLARS OF THE NIST CYBERSECURITY FRAMEWORK.



4.1. *IDENTIFY* which provides the capability of developing the operators understanding in managing their cybersecurity risk to systems, assets, data, and capabilities.

4.2. *PROTECT/PREVENT* for capability to enable operators to proactively anticipate new attack types against the current infrastructure systems and information, and to proactively prioritise and aggress exposure. By identified risks through controls to limit or contain the impact of a potential cyber security event.

4.3. *DETECT* by developing or implementing capabilities designed to find attacks that have evaded the preventative layer, with the goal of reducing potential cyber security events in a timely manner.

4.4. *RESPOND* to provide the functions required to investigate and remediate issues discovered through detective activities, to provide root cause, analysis and to recommend new preventative measure to minimise events and to incorporate lessons learned into new strategies.

4.5. *RECOVER* to provide the capability to develop and implement the appropriate activities to maintain plans for resilience and to restore ant impacted service due to cybersecurity event.

5. BASED ON THE NIST FRAMEWORK THE CYBERSECURITY PROGRAMME SHOULD ADDRESS THE FOLLOWING AREAS:

5.1. Establishment of Leadership and Governance structure to support cyber/information security requirements

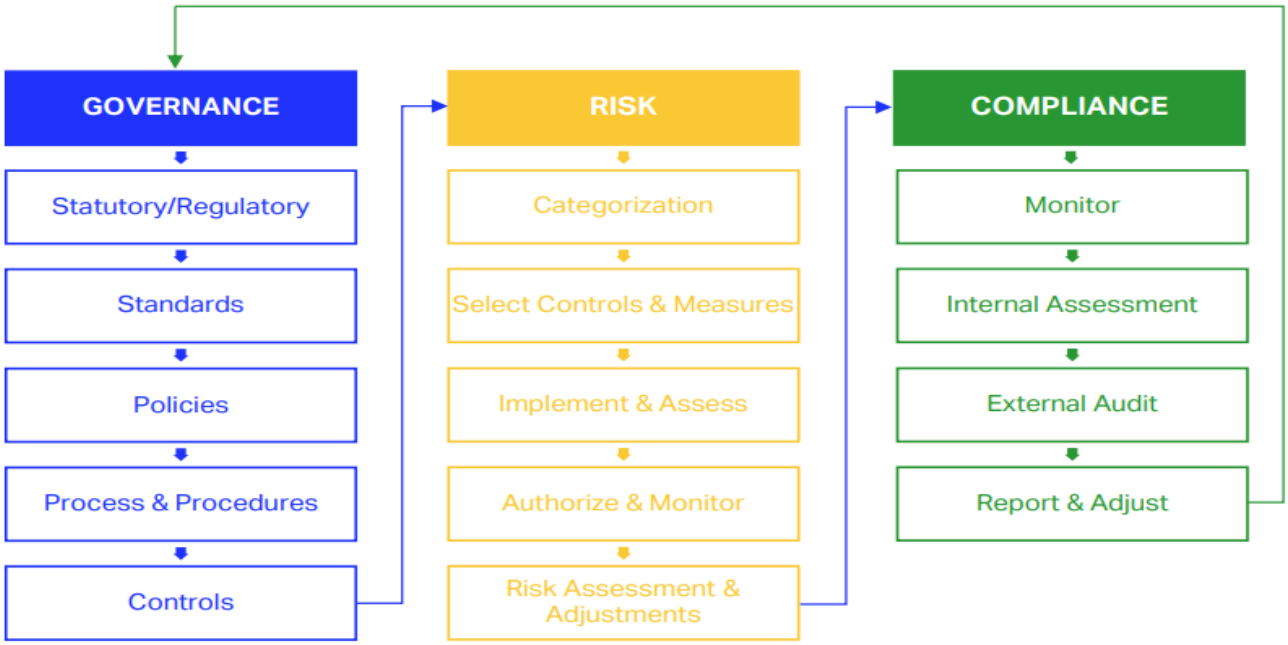
5.1.1 Leadership and Management

a. Formulation and the development of strategies to allow for the engagement of issues, and to foster dialogue with the Authority, third party providers and those that form part of the aviation value chain to strengthen awareness and to improve preparedness.

b. An effective cybersecurity culture is depended on the commitment of every person in the organization, staring with senior management. The senior management are to provide their full commitment to cybersecurity culture, always and across all activities, strategies, policies and organisational objectives
c. To adopt a cybersecurity risk management approach to aid in decision making and to ensure accountability with the purpose on developing cybersecurity culture.

5.1.2 Governance, Risk and Compliance (GRC) framework

a. Governance with the purpose of providing a framework for policy and process formulation, to support management and operational structures.
b. Risk to provide appropriate steps to identify, assess and understand the operators CSIAD security risks. This includes an overall organisational approach to risk management.
c. Compliance to ensure compliance with the ICAO, national, authority, industry and technology requirements rule set in information security and cybersecurity domain.



5.1.3 Information Security Management System (ISMS)

a. The adoption of a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organisation's information security (CIA) to achieve business objectives.

5.2. IDENTIFY

5.2.1 Assets Management

a. The data, personnel, devices, systems, and facilities must be identified and managed consistent in line with their criticality level, business objectives and the operator's risk strategy.

5.2.2 Risk Management

a. To perform risk assessment through the identification of assets and their attack path, vulnerability and the extend of risk exposure.

b. The operator to understand the cybersecurity risk within its operations (including mission, functions, image, or reputation), operator assets, and individuals, including system-of-system aspects resulting from dependencies.

5.2.3 Information Sharing

a. The operator to obtains and shares its threat intelligence, vulnerability, and attack/incident information activities, with internal and external parties to encourage collaboration.
b. Application of the Traffic light protocol to guide for systematic coordination

COLOUR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED
RED	Not for disclosure, restricted to participants only. Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP: RED information is limited to those present at the meeting. In most circumstances, TLP: RED should be exchanged verbally or in person.
AMBER	Limited disclosure, restricted to participants' organizations. Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
GREEN Low Risk	Limited disclosure, restricted to the community. Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP: GREEN information may not be released outside of the community.
WHITE	Disclosure is not limited. Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,	TLP: WHITE information may be distributed without restriction.

5.2.4 Supply Chain Management

a. The ability to identify and manage those involved in the entire aviation value chain to determine the operator's priorities, constraints, risk tolerances, and assumptions to support risk decisions associated with managing supply chain risk.
b. The operator to formulate processes and procedures to identify, assess and manage supply chain risks within its extended value chain.

5.3. PROTECT

5.3.1 Identity Management and Access Control

a. Access to physical and logical assets; and its associated facilities must be limited to authorised users, processes, and devices. These serve to respond, to ensure consistency with the risk results obtained.

5.3.2 Human Centric Security

a. With the purpose of providing cybersecurity awareness and training to the operator's personnel and its partners, to support their information security and cybersecurity outcomes.

5.3.3 Protective Technology

a. Technical security solutions are to be managed to ensure that security and resilience of systems and assets are consistent with related policies, procedures, and agreements.
b. Systems and processes designed to be sensitive to the additional workload created by cybersecurity requirements

5.3.4 Training and Awareness

a. The operator's staff to have adequate training to support and inform protection method, together with the provision of related policies, procedures, and agreements.

5.4. DETECTION

5.4.1 Anomalies and Events

a. Anomalous activity with the intention of detecting activities in a timely manner for the potential impact of events must be understood.
b. The operator to monitors the security status of the networks and systems supporting the operation of critical systems to detect potential security problems and to track the ongoing effectiveness of protective security measures.

5.4.2 Continuous Monitoring

a. This involves monitoring of information systems and assets at discrete intervals to identify any cybersecurity events, with the objective of verifying the effectiveness of the protective measures.

5.5. RESPOND

5.5.1 Response Planning

a. Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events

5.5.2 Continuous Improvement

a. The safeguarding of the aviation ecosystems is depended on application of cyber risk management practices, with the purpose of identifying and changing deficiencies to achieve cyber resiliency.
b. The adoption of the PLAN-DO-CHECK -ACT approach to the effectiveness and support of the cyber risk management practice.
c. Lesson learned recording of steps taken to understand the root causes and to ensure appropriate remediating action is taken to safeguard against future incidents.

5.5.3 Cybersecurity Culture

a. An integral part of the operators and its staff based on the operators set of knowledge, norms, values which the staff directly reflect their behaviors in dealing with the information technology and protection of critical system, inform, assets and data encompassing the entire life cycle

5.5.4 Mitigation

a. Activities/Evaluation of effective mitigation strategies to inform the selection of preventative measures to respond, effect and possible eradication of the incident.
b. The maintenance and managements of an operator risk register to inform the prioritisation of risk

5.6. RECOVER

5.6.1 Incident Management

a. With the aim of ensure continuity of essential functions in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise to be established.

5.6.2 Recovery Planning

a. Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.

5.6.3 Communication

a. Restoration of activities to be coordinated with internal and external parties, considering the interconnectedness and interdependencies that exist within aviation ecosystem.
b. To effective communication, the skills required as part of robust cybersecurity culture namely: active listening; adapting communication style to different audience and situation and clarity of communication

5.6.4 Reference to Information security, Cybersecurity, and risk document it is essential to address the entire scope of cybersecurity, as it continuously evolving with the goal of maintaining the confidentiality, integrity, availability, authentication, authorisation and non-repudiation within the entire aviation operation

DEVELOPED BY:		
	DIKELEDI MZIMBA	28 MARCH 2022
SIGNATURE OF AVSEC: RS	NAME IN BLOCK LETTERS	DATE
REVIEWED & VALIDATED BY:		
	MARCHE` ARNOLD	28 MARCH 2022
SIGNATURE OF ACTING M: OS	NAME IN BLOCK LETTERS	DATE
APPROVED BY:		
	LUVUYO LULAMA GQEKE	28 MARCH 2022
SIGNATURE OF E: AVSEC	NAME IN BLOCK LETTERS	DATE

END