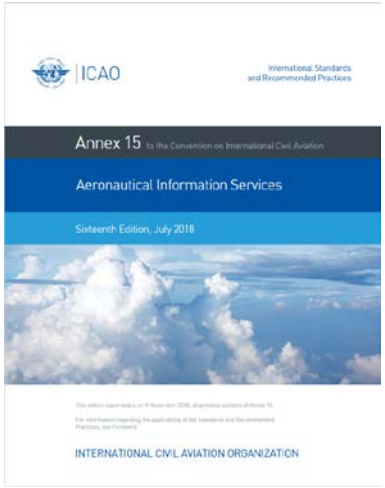
ICAO UNITING AVIATION

Technical infrastructure and information security framework

Annex 15 – Aeronautical Information Services



5.4 Distribution services

…

5.4.3 Data set information services

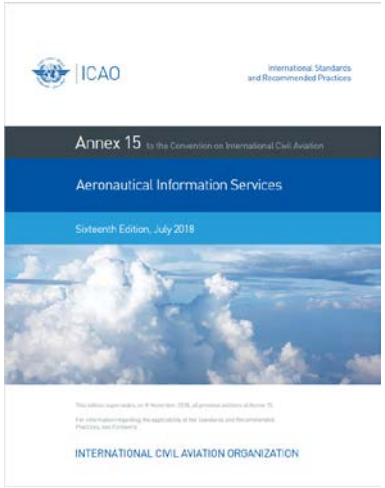
5.4.3.1 **Recommendation.**— When provided, the digital data sets specified in 5.3 should be made available through information services.

Note 1.— In the context of system-wide information management, the notion of information service addresses machine-to-machine interaction in a service-oriented architecture.

Note 2. — Procedures on information services are contained in the Procedures for Air Navigation Services - Information Management (PANS-IM, Doc 10199).

Note 3.— Guidance material on information services can be found in the Manual on System-wide Information Management Implementation (Doc 10203).

Annex 15 – Aeronautical Information Services



5.4 Distribution services

…

5.4.3 Data set information services

5.4.3.1 **Recommendation.**— When provided, the digital data sets specified in 5.3 should be made available through information services.

Note 1.— In th[illegible]ontext of system-wide information management, the notion of informa[illegible]ice addresses machine-to-machine interaction in a service-orient[illegible]

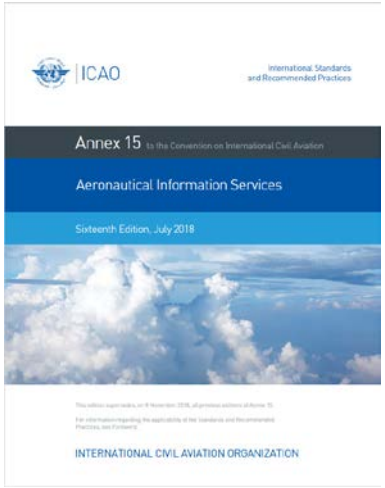
Note 2 Proce[illegible] (PANS[illegible]

Note 3 Manua[illegible] 10203[illegible]

5.3.1.1 Digital data shall be in the form of the following data sets: a) AIP data set; b) terrain data sets; c) obstacle data sets; d) aerodrome mapping data sets; and e) instrument flight procedure data sets.

Note.— Detailed specifications concerning the content of the digital data sets are contained in the PANS-AIM (Doc 10066).

Annex 15 – Aeronautical Information Services



5.4.3.1.1 A data set information service shall provide, as a minimum, the ability to query and retrieve, as a whole, each of the digital data sets specified in 5.3.

5.4.3.1.2 **Recommendation.**— A data set information service should provide the ability to query and retrieve selected elements of the digital data sets specified in 5.3.

Note.— Guidance material on how to query digital data sets is contained in the Aeronautical Information Services Manual (Doc 8126), Part IV.

5.4.3.1.3 **Recommendation.**— A data set information service should provide the option to subscribe to notifications on data set updates.

PANS – Information Management (Doc 10199)

6 TECHNICAL INFRASTRUCTURE

6.1 GENERAL

Information services shall be provided and consumed using a technical infrastructure based on the Internet Protocol Suite (IPS).

6.2 INTERFACE BINDINGS

6.2.1 Information services **use interface bindings** to interact with the technical infrastructure.

Note.— See Doc 10203 for more information on interface bindings.

PANS – Information Management (Doc 10199)

6.2.2 Interface bindings shall be based on **standardized and widely used and supported protocols**.

Note 1.— These protocols provide the necessary capabilities to enable information service providers and consumers to exchange information via interoperable services applying loose coupling principles between systems.

Note 2.— Two systems that implement the same interface binding are technically interoperable, and therefore capable to connect and to exchange information.

6.2.2.1 In order to ensure interoperability, if information service providers and consumers are **using different protocols**, both parties shall ensure that **lossless mediation between protocols has been established.**

Note 1.— Lossless mediation means that the message and its properties are preserved in the bi-directional conversion between two protocols.

Note 2.— Guidance on lossless mediation, including the required application property names and types, can be found in Doc 10203.

PANS – Information Management (Doc 10199)

6.2.3 **Information service providers should manage interface bindings to consolidate the potentially large number of technologies that could be used for implementing interfaces between systems and to maintain flexibility in relation to the opportunities of emerging potential technologies**.

6.2.4 Information services should use defined interface bindings in accordance with 6.2.2 and 6.2.3.

Note 1.— Doc 10203 provides further guidance on functional capabilities, loosely coupling, interface bindings and interoperable mediation between protocols.

Note 2.— An example of a specification on interface bindings is shown in EUROCONTROL Specification for SWIM Technical Infrastructure (TI) Yellow Profile (EUROCONTROL-SPEC-170).

The network

- IP based and independent from the technical infrastructure
- Outside of the scope of SWIM. However, the selection of an infrastructure impacts:
  - the feasibility and selection of Message Exchange Patterns (MEPs)
  - the degree of synchrony that can be assumed between interacting systems
  - the reliance on intermediary technical capabilities to support indirect or asynchronous interactions
- The level of connectivity available between participants has a direct impact on how services can be implemented and which MEPs can be effectively used across domains.

The technical infrastructure

- Impacted by the connectivity at the network level
- Message exchange patterns like request/reply or publish/subscribe should be determined based on business needs
- In SWIM, information services are made available through Application Programming Interfaces (APIs) which define the functional contract between information service providers and consumers.
- APIs are implemented through bindings, which specify the technical realization of the service, which includes:
  - Message format (JSON, XML, etc.)
  - Transport protocol (HTTP, AMQP, etc.)
  - Security mechanisms
  - Endpoint structure

No single implementation approach is suitable for all SWIM services or operational environments. Connectivity conditions, security requirements, operational constraints, and information exchange needs may lead to different implementation choices. However, maintaining a common architectural approach that preserves SWIM principles is essential to achieving global interoperability.

PANS – Information Management (Doc 10199)

6.3 INFORMATION SECURITY FRAMEWORK

6.3.1 System-wide information management stakeholders processing, storing, consuming or transferring information shall implement an information security framework, designed to ensure the confidentiality (when needed), integrity and availability of the information and information services.

6.3.2 The information security framework shall apply to the IPS-based network, technical infrastructure, information, information service and applications that process, use or distribute information in an integrated manner.

Note.— Guidance on how to implement the information security framework, as part of another framework or an independent framework, is provided in Doc 10204.

PANS – Information Management (Doc 10199)

6.3.3 Information service providers shall classify information according to defined information security categories to ensure a mutual understanding of the level of protection of the information exchanged.

Note.— See Doc 10204 for classification of information in the defined information security categories.

6.3.4 System-wide information management stakeholders should implement information security requirements commensurate with the information security category determined in 6.3.3.

Note.— For more information on commensurate information security requirements, see Doc 10204.

PANS – Information Management (Doc 10199)

6.3.5 Information service consumers shall assess the impact of the loss of confidentiality, integrity and availability of the information on safety to determine the information security category required for the operational use of the information.

Note 1.— The loss of confidentiality, integrity and availability of the information may impact safety.

Note 2.— See Doc 10204 for the assessment of the impact of the loss of confidentiality, integrity and availability of the information on safety and classification of information in information security categories.

Manual on Aviation Information Security (Doc 10204)

- To build trust between stakeholders exchanging information by ensuring a common understanding of the level of protection of that information in terms of confidentiality, integrity and availability.
- An approach to address risks in an interconnected manner and to determine the level of confidentiality, integrity and the availability of protection required for information.
  - Based on the level of protection required, a series of tiered information security objectives based on NIST 800-53 and ISO 27001 in areas that relate to information security management are described.
- Specific aspects of the framework to implement these objectives (SMS, SeMS or ISMS) is out of scope.

Manual on Aviation Information Security (Doc 10204)

Information system owners should assess risks following the risk approach described in Chapter 2, 2.2.2 to determine the level of protection required (basic, intermediate or advanced) for each area.

Note.— The level of protection can be different for each area (that is, confidentiality, integrity and availability).

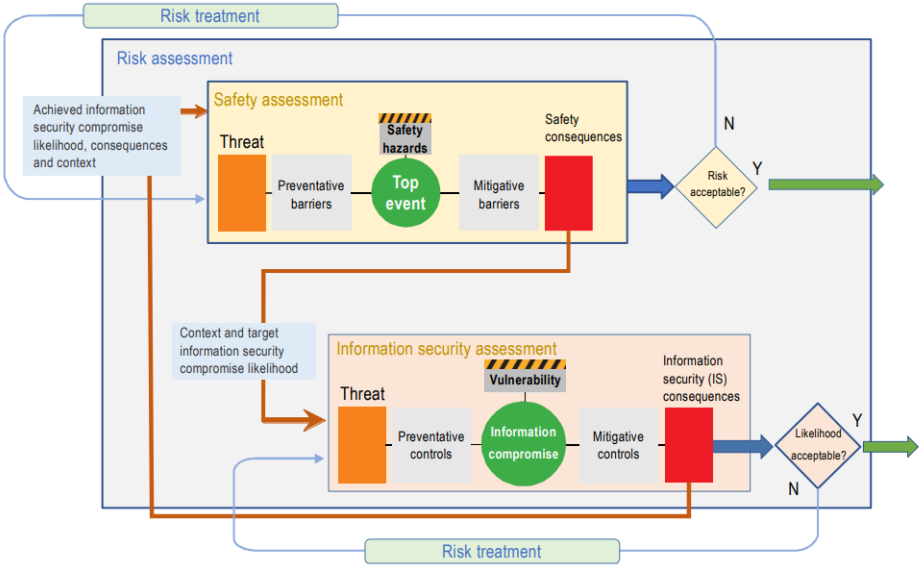


Figure 2-1. Information security risk assessment in the context of safety consequences

Manual on Aviation Information Security (Doc 10204)

Once the determination is made of the level or levels of protection required (basic, intermediate, or advanced) for the information system or systems, information system owners can then identify the level of performance needed and review the suggested tools and best practices available to achieve it.

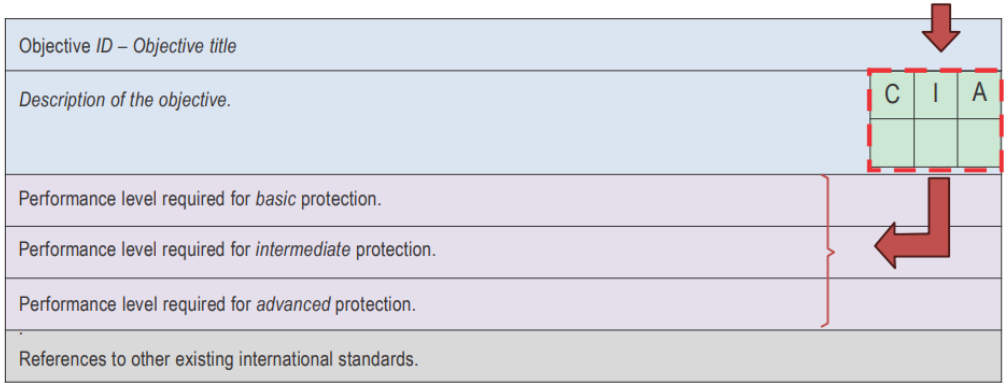


Figure 1-1. Objectives template

Manual on Aviation Information Security (Doc 10204)

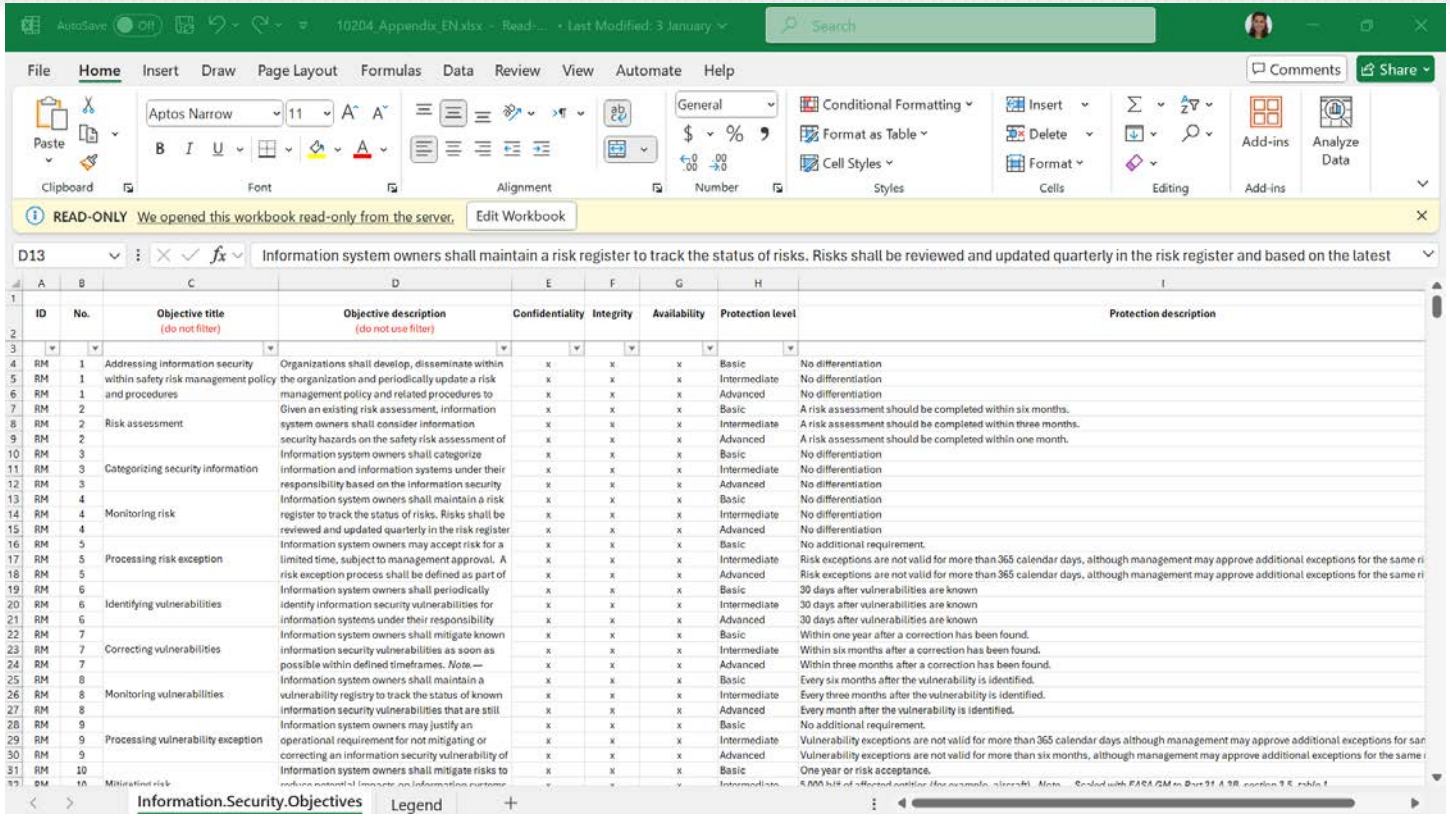
- Chapter 2 - Risk Management
- Chapter 3 - Information security assessment and authorization
- Chapter 4 - Identity and access management
  - Doc 10169 Aviation Common Certificate Policy
- Chapter 5 - Information system configuration and management
- Chapter 7 - Continuity planning
- Chapter 8 - Information security planning
- Chapter 9 - Configuration management
- Chapter 11 - Information system maintenance
- Chapter 13 - Supply chain risk management
- Chapter 14 - Media protection
- Chapter 15 - Physical and environmental security
- Chapter 16 - Personnel security

Manual on Aviation Information Security (Doc 10204)

Objective IAM.5 – Credential management			
	C	I	A
– Organizations shall have a credential management process to: a) identify the individual, group, role, or information system sponsor receiving the credentials; b) ensure the credentials have sufficient strength for the intended use; c) establish and change the default credential contents; and d) provide, manage, and de-provide credentials. – At a minimum, credentials should be: a) assigned and personalized to individuals, groups, roles, or information system sponsors; b) renewed periodically; c) replaced if lost or stolen; and d) deactivated upon separation events.	x	x	
Basic protection level: Level 1 credentials should not be used.			
Intermediate protection level: Level 1 or Level 2 credentials should not be used.			
Advanced protection level: Level 1, Level 2 or Level 3 credentials should not be used.			
References: NIST 800-53: AC-2, IA-5 and ISO 27001: A.9.2.4, A.9.4, A.9.4.1, A.9.4.2, A.9.4.3.			

Table 4-1. Identity assurance levels

Level	Description
Level 0	No identity proofing is required, however, basic access control is supported (for example, a simple password). Level 0 provides little or no confidence in the asserted identity's validity.
Level 1	Identifying materials or information are required and may be provided in person or remotely. Level 1 provides single factor remote network authentication (for example, what I know or what I have). Level 1 provides some confidence in the asserted identity's validity.
Level 2	Identifying materials or information are required and may be provided in person or remotely. Level 2 provides multi-factor remote network authentication (for example, what I know and what I have) and requires proof of possession of a key through a cryptographic protocol. Level 2 provides high confidence in the asserted identity's validity.
Level 3	Identifying materials or information are required and must be provided in person or remotely. Level 3 provides multi-factor remote network authentication (for example, what I know and what I have) and requires proof of possession of a key through a cryptographic protocol based on a hardware token with Federal Information Processing Standards (FIPS) 140-2 Level 2 overall with at least FIPS 140-2 Level 3 physical security. Level 3 provides very high confidence in the asserted identity's validity.



10204 Appendix EN.xlsx - Read-... • Last Modified: 3 January

READ-ONLY We opened this workbook read-only from the server. Edit Workbook

D13: Information system owners shall maintain a risk register to track the status of risks. Risks shall be reviewed and updated quarterly in the risk register and based on the latest

ID	No.	Objective title (do not filter)	Objective description (do not use filter)	Confidentiality	Integrity	Availability	Protection level	Protection description
RM	1	Addressing information security	Organizations shall develop, disseminate within	x	x	x	Basic	No differentiation
RM	1	within safety risk management policy	the organization and periodically update a risk	x	x	x	Intermediate	No differentiation
RM	1	and procedures	management policy and related procedures to	x	x	x	Advanced	No differentiation
RM	2		Given an existing risk assessment, information	x	x	x	Basic	A risk assessment should be completed within six months.
RM	2	Risk assessment	system owners shall consider information	x	x	x	Intermediate	A risk assessment should be completed within three months.
RM	2		security hazards on the safety risk assessment of	x	x	x	Advanced	A risk assessment should be completed within one month.
RM	3		Information system owners shall categorize	x	x	x	Basic	No differentiation
RM	3	Categorizing security information	information and information systems under their	x	x	x	Intermediate	No differentiation
RM	3		responsibility based on the information security	x	x	x	Advanced	No differentiation
RM	4		Information system owners shall maintain a risk	x	x	x	Basic	No differentiation
RM	4	Monitoring risk	register to track the status of risks. Risks shall be	x	x	x	Intermediate	No differentiation
RM	4		reviewed and updated quarterly in the risk register	x	x	x	Advanced	No differentiation
RM	5		Information system owners may accept risk for a	x	x	x	Basic	No additional requirement.
RM	5	Processing risk exception	limited time, subject to management approval. A	x	x	x	Intermediate	Risk exceptions are not valid for more than 365 calendar days, although management may approve additional exceptions for the same ri
RM	5		risk exception process shall be defined as part of	x	x	x	Advanced	Risk exceptions are not valid for more than 365 calendar days, although management may approve additional exceptions for the same ri
RM	6		Information system owners shall periodically	x	x	x	Basic	30 days after vulnerabilities are known
RM	6	Identifying vulnerabilities	identify information security vulnerabilities for	x	x	x	Intermediate	30 days after vulnerabilities are known
RM	6		information systems under their responsibility	x	x	x	Advanced	30 days after vulnerabilities are known
RM	7		Information system owners shall mitigate known	x	x	x	Basic	Within one year after a correction has been found.
RM	7	Correcting vulnerabilities	information security vulnerabilities as soon as	x	x	x	Intermediate	Within six months after a correction has been found.
RM	7		possible within defined timeframes. *Note.*—	x	x	x	Advanced	Within three months after a correction has been found.
RM	8		Information system owners shall maintain a	x	x	x	Basic	Every six months after the vulnerability is identified.
RM	8	Monitoring vulnerabilities	vulnerability registry to track the status of known	x	x	x	Intermediate	Every three months after the vulnerability is identified.
RM	8		information security vulnerabilities that are still	x	x	x	Advanced	Every month after the vulnerability is identified.
RM	9		Information system owners may justify an	x	x	x	Basic	No additional requirement.
RM	9	Processing vulnerability exception	operational requirement for not mitigating or	x	x	x	Intermediate	Vulnerability exceptions are not valid for more than 365 calendar days although management may approve additional exceptions for san
RM	9		correcting an information security vulnerability of	x	x	x	Advanced	Vulnerability exceptions are not valid for more than six months, although management may approve additional exceptions for the same
RM	10		Information system owners shall mitigate risks to	x	x	x	Basic	One year or risk acceptance.
RM	10	Mitigating risk	reduce potential impacts on information systems	x	x	x	Intermediate	5,000 hull of affected entities (for example, aircraft). Note.— Scaled with EASA GM to Part 21.A.3B, section 3.5, table 1

Information.Security.Objectives | Legend

PANS – Information Management (Doc 10199)

5.2.1 Information service providers shall provide information service metadata through information service overviews.

5.2.2 Information service overviews shall be structured using the metadata fields in Table 5-1. This practice facilitates discoverability of information services and enables information service consumers to compare different information services.

5.2.3 Information service providers shall provide a complete description of all metadata fields in the information service overview for each version of an information service.

Field name	*Requirements*	*Field schema*	*Example*
Source of information	Information service providers should specify the sources of information exchanged. Information service providers should also provide information on any subsequent modifications applied in order to provide information service consumers with background on information sources and modifications. If an information service provider does not make the source of information available, the *source of information* metadata field shall specify "NIL".	Free text *or* NIL	*DONLON Airport Operator*
Information security category	Information service providers shall indicate the information security category to provide information service consumers with an understanding of the level of protection of the information. The information security category shall be expressed as one of the following: a) none; b) basic; c) intermediate; or d) advanced. *Note.— More information is provided in the* Manual on Information Security *(Doc 10204).*	None *or* Basic *or* Intermediate *or* Advanced	*Intermediate*

Manual on Aviation Information Security (Doc 10204)

- Clarification: The framework does not prescribe a specific ISMS, SMS, or SeMS implementation, but rather provides a common basis for determining and communicating the required level of protection for information exchanged through SWIM.
- Second edition on its way!
  - Chapter 6 - Information security incident response and recovery
  - Chapter 10 – Continuous Monitoring
  - Clarification to Chapter 4 – Identity management and monitoring
  - New Appendix B: Template to facilitate the application of the iterative joint (safety and information security) risk assessment process.
- Target date for publication: September 2026

ICAO


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