CYBER COMPLIANCE FRAMEWORK FRANCE

VERSION 3

Implementing Regulation (EU) 2015/1998
Delegated Regulation (EU) 2022/1645
Implementing Regulation (EU) 2023/203

Direction de la sécurité de l'aviation civile
Direction de programme cybersécurité
Version n°3.0 July 11th 2025

Table of contents

Information

This document prepared by the civil aviation authority of France (DSAC) and the civil aviation safety organisation (OSAC) presents the Cyber Compliance Framework France (3CF[1]) for civil aviation. This document marked TLP:CLEAR may therefore be freely used within the air transport community and provided that its origin (source and date of the last update) is mentioned.

For any comments or suggestions regarding the Cyber Compliance Framework France (3CF) please contact:

- DSAC at: dp-cyber-dsac.bf@aviation-civile.gouv.fr, or
- OSAC by requesting a modification. The procedure is available at: https://documentation.osac.aero/.

Revision history

Version	Date	Modifications
Intermediate Version	June 30th 2021	Creation of the document
Version 1	Sept. 3rd 2021	- Changes: ○ § 1. Introduction ○ § 2. Support Approach ○ § 4.1.4. Personnel and Competence ○ § 5.4.4.1. Sources of non-conformities ○ Appendix 3: Regulatory Compliance Grid, - Additions: ○ § 5.1.3. Training ○ Appendix 2: Compliance Levels and Provisions of 3CF
Version 2	April 30th 2024	Overhaul of the document to integrate the AMC of Part IS regulation
Version 3.0	July 11th 2025	- Changes: ○ § 1.2. Scope ○ § 1.3. Equivalence between regulatory frameworks ○ §2. General presentation of the document ○ §4.1. Establishing the context ○ §4.4.1. Detection of information security incidents ○ § 5.1.3.2. Personnel abroad ○ §8. Documentation ○ Annexe IV: Compliance matrix ○ Annexe V: Definitions ○ Annexe VII: References - Additions: ○ All: Regulatory references ○ § 3.3. Common responsible person ○ § 4.2.2. Organisation addressed by Part ATM/ANS.OR ○ § 4.2.4. Organisation addressed by Part ATM/ANS.OR ○ § 4.4.5. Notification to the competent authority ○ § 4.5.1.2.1. Notification to DOA ○ §6.2.2. Response to findings notified by the competent authority ○ § 6.4. Changes to the ISMS ○ §7. Record keeping ○ Annexe I: Best practices ○ Annexe II: Security essential functions ○ Annexe III: Safety essential functions ○ Annexe VI: Acronyms

[1] 3CF is the French acronym and will be kept as is in this document.

1. Introduction

1.1. Objective of the document

This document is a guide that provides a unique framework of provisions to assist organisations in complying with:

- Implementing Regulation (EU) 2015/1998 [1] as amended by Commission Implementing Regulation (EU) 2019/1583 of September 25, 2019, laying down detailed measures for the implementation of common basic standards on civil aviation security concerning cybersecurity measures, and/or,
- Part-IS regulations:
  - Commission Delegated Regulation (EU) 2022/1645 [2] of July 14, 2022, laying down detailed rules for the implementation of Regulation (EU) 2018/1139 of the European Parliament and of the Council with regard to requirements for the management of information security risks that may affect aviation safety,
  - Commission Implementing Regulation (EU) 2023/203 [3] of October 27, 2022, laying down detailed rules for the implementation of Regulation (EU) 2018/1139 of the European Parliament and of the Council with regard to requirements for the management of information security risks that may affect aviation safety.

1.2. Scope

1.2.1. Operators holding a security approval.

This document is intended for **aerodrome operators** and **air carriers** subject to Implementing Regulation (EU) 2015/1998 [1].

1.2.2. Organisations holding a safety approval or certificate.

This document is intended for the following organisations:

Applicable	Exempted
Design organisations (DOA) subject to Subparts G and J of Section A of Annex I (Part 21) to Regulation (EU) No 748/2012 [4]	Design organisations that are **solely involved in the design of ELA2 aircraft** as defined in Article 1(2), point (j) of Regulation (EU) No 748/2012 [4]
Production organisations (POA) subject to Subparts G and J of Section A of Annex I (Part 21) to Regulation (EU) No 748/2012 [4]	Production organisations that are **solely involved in the production of ELA2 aircraft** as defined in Article 1(2), point (j) of Regulation (EU) No 748/2012 [4]
Aerodrome operators and apron management service providers subject to Annex III 'Part Organisation Requirements (Part-ADR.OR)' to Regulation (EU) No 139/2014 [5]	
Maintenance organisations subject to Section A of Annex II (Part-145) to Regulation (EU) No 1321/2014 [6]	Maintenance organisations **solely involved in the maintenance of aircraft** in accordance with Annex Vb (Part-ML) to Regulation (EU) No 1321/2014 [6]
Continuing airworthiness management organisations (CAMOs) subject to Section A of Annex Vc (Part-CAMO) to Regulation (EU) No 1321/2014 [6]	CAMO **solely involved in the continuing airworthiness management of aircraft** in accordance with Annex Vb (Part-ML) to Regulation (EU) No 1321/2014 [6]
Air operators subject to Annex III (Part-ORO) to Regulation (EU) No 965/2012 [7]	Air operators **solely involved in the operation of** any of the following: - an **ELA 2 aircraft** as defined in Article 1(2), point (j) of Regulation (EU) No 748/2012 [4], - **single-engine propeller-driven aeroplanes** with a Maximum Operational Passenger Seating Configuration of 5 or less that are not classified as complex motor-powered aircraft, when taking off and landing at the same aerodrome or operating site and operating under Visual Flight Rules (VFR) by day rules, - **single-engine helicopters** with a Maximum Operational Passenger Seating Configuration of 5 or less that are not classified as complex motor-powered aircraft, when taking off and landing at the same aerodrome or operating site and operating under VFR by day rule
Approved training organisations (ATOs) subject to Annex VII (Part-ORA) to Regulation (EU) No 1178/2011 [8]	**ATOs solely involved:** - in training activities of ELA2 aircraft **as defined in Article 1(2), point (j) of Regulation (EU) No 748/2012** [4], - theoretical training

Aircrew aero-medical centres subject to Annex VII (Part-ORA) to Regulation (EU) No 1178/2011 [8]	
Flight simulation training device (FSTD) operators subject to Annex VII (Part-ORA) to Regulation (EU) No 1178/2011 [8]	FSTD operators **solely involved in the operation of FSTDs for ELA2 aircraft** as defined in Article 1(2), point (j) of Regulation (EU) No 748/2012 [4]
Air traffic controller training organisations (ATCO TOs) subject to Annex III (Part ATCO.OR) to Regulation (EU) 2015/340 [9]	
ATCO aero-medical centres subject to Annex III (Part ATCO.OR) to Regulation (EU) 2015/340 [9]	
Air navigation service providers (ANSP) subject to Annex III (Part-ATM/ANS.OR) to Implementing Regulation (EU) 2017/373 [10]	- **Air navigation service providers holding a limited certificate** in accordance with point ATM/ANS.OR.A.010 of Annex III (Part-ATM/ANS.OR) to Implementing Regulation (EU) 2017/373 [10] - **Flight information service providers declaring their activities** in accordance with point ATM/ANS.OR.A.015 of Annex III (Part-ATM/ANS.OR) to Implementing Regulation (EU) 2017/373 [10]
Flight procedure design organisations (FPD) subject to Annex III (Part-ATM/ANS.OR) to Implementing Regulation (EU) 2017/373 [10]	
U-space service providers and **single common information service providers** subject to Implementing Regulation (EU) 2021/664 [11]	

1.2.3. Dispensation from certain Part-IS requirements

Regulations (EU) n°2023/203 and (EU) n°2022/1645-IS.I/D.OR 200 (e), provide for the competent authority to dispense an organisation from applying certain requirements of Part-IS, for a limited period of time. In particular, the organisation has the option of not implementing an Information Security Management System (ISMS) if it demonstrates, through a formalized risk analysis as defined in points IS.I/D.OR.205, that it presents a limited risk to aviation safety in relation to the overall exposure in its daily activity.

The framework for this dispensation from the application of Part-IS and the eligibility criteria are specified in METEOR DSAC communications [12] and in the BI OSAC 2025-03 [13].

Organisation potentially eligible for this dispensation are:

- For organisation overseen by DSAC:
  - Specialised Organisation (SPO) and Non-commercial specialised operations with complex aircraft (NCC),
  - Certain:
    - Approved training organisation (ATO),
    - Flight simulator training device operators (FSTD),
    - Air traffic controller training organisation (ATCO-TO),
    - Flight procedure design organisation (FPD),
    - ATCO aeromedical centres,
    - U-Space service providers.
  - Less complex CAT operators.
- For organisation overseen by OSAC, the dispensation eligibility criteria depend on the type of activity:
  - Part-21G: Production only of components that do not have a major "safety" function,
  - Part-145: Work only on components that do not have a major "safety" function or do not contribute to structural integrity,
  - Part-CAMO: CAMO approvals managing only:
    - the aircraft fleet of an operator considered potentially dispensable by the DSAC,
    - aircraft in storage or only implementing Subpart I of Regulation (EU) No 1321/2014 [6].

1.3. Equivalence between regulatory frameworks

The terms and conditions of the equivalences between the Part-IS regulations [2,3] and regulation (EU) 2015/1998 [1] on the one hand and the French transposition of the NIS 2 Directive [44] on the other hand will be specified in version 3.1 of the Cyber Compliance Framework France.

2. General presentation of the document

2.1. Unique framework

Considering the multiplicity of regulations, redundancy of certain requirements, and the constraints on human and financial resources exacerbated by the current crisis, this document aims to provide operators with a Cyber Compliance Framework France (3CF). Its objective is to streamline the various regulatory provisions applicable to civil aviation in France to facilitate their implementation through a single reference framework (3CF).

The 3CF aims to:

- facilitate compliance with:
  - regulation (EU) No 2015/1998 [1] concerning information security that may affect aviation security,
  - the Part-IS framework [2,3] concerning information security that may affect aviation safety.
- ensure coherence without guaranteeing compliance with national provisions such as:
  - the « air transport » sectoral order [14] resulting from Article 22 of the Military Programming Law,
  - the decree and orders [15] resulting from the law transposing the Network Information Security Directive.

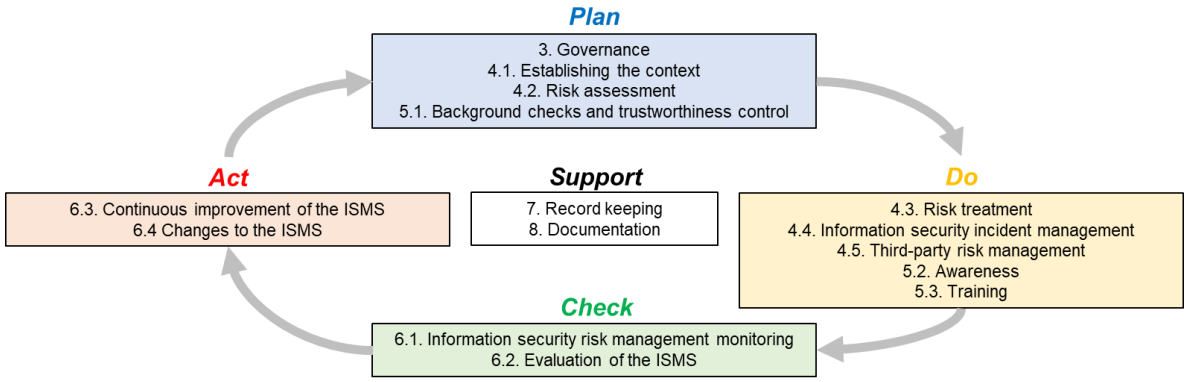
Furthermore, it is inspired by best practices such as:

- ISO 27001 standard [16] related to information security management systems,
- Guidance and methodologies from the National Agency for Information Systems Security (ANSSI)[2],
- International and European works conducted by ICAO, EASA and EUROCAE.

Indeed, although the different regulatory frameworks do not concern the same areas of air transport: national protection, economic security, civil aviation security, or civil aviation safety, they rely on cross-cutting principles and methods for information security. The unique framework (3CF) aims to rationalize these requirements into a single framework.

2.2. Structure

In the context of implementing an information security management system, the document chapters should be read accordingly:



2.3. Use

For organisations required to comply:

- with both regulations, the entire document should be considered, and the scope covers both aviation security and safety,
- solely with the Part-IS framework [2,3], the whole document should be considered, and the scope covers only aviation safety,
- solely with Regulation (EU) No 2015/1998 [1], the provisions outlined in chapters §4.1, §4.2, §4.3, §4.4.4, §4.5.1.1, §5., §6.1 and §8.1 should be considered and the scope covers only aviation security.

For each provision, an insert recalls the regulatory reference among:

- **Part-IS** [2,3],
- the elements related to the security regulation**: RUE 2015/1998** [1], **the decree of September 11th 2013** [38] relating to civil aviation security measures and the **French code of transport** [39],
- or **both.**

[2] ANSSI publications

The following elements are included in the appendix:

- a list of best practices for implementing the provisions of this document,
- lists of essential functions for risk assessment,
- the compliance matrix specifying the provisions of the document that apply as appropriate,
- definitions of the key terms used in the document,
- acronyms used in the document,
- references to productions mentioned in the document.

2.4. Implementation

The application of Part-IS is a condition for maintaining organisations certificates/approvals.

Part-IS specifically requires the implementation of an Information Security Management System (ISMS) whose principles are similar to those of a Safety Management System (SMS) as required by Part-21, ADR, CAMO, 145, ORO, ORA, ATCO, and ATM/ANS regulations.

Although no regulation requires the integration of management systems, especially ISMS and SMS, organisations may choose to implement an integrated system covering both aviation safety and information security.

Depending on the organisation structure, this option can optimize resources and the overall effectiveness of Part-IS implementation, by supplementing or adapting existing elements of the safety management system where relevant (organisations, policies, procedures, etc.). In any cases, the organisation ensures that ISMS is coordinated with SMS.

3. Governance

3.1. Commitment of the Accountable Manager

IS.I/D.OR 200 a) 1)

The Accountable Manager commits to implementing appropriate protection measures against the breach of confidentiality, integrity, availability, and authenticity of information that could lead to aviation safety issues. To this end, the Accountable Manager commits to implementing an Information Security Management System (ISMS) aimed at identifying, implementing, operating, monitoring, reviewing, maintaining, and improving the management of information security risks related to aviation safety.

The commitment from the Accountable Manager is formalised and integrated or referenced in:

- the information security management system manual or,
- the safety management system manual of the organisation.

3.2. Information security policy

3.2.1. Strategy and objectives of information security

IS.I/D.OR 200 a) 1)

The Accountable Manager defines and approves an information security policy that:

- specifies the scope of the ISMS as defined in §4.1.
- includes:
  - a strategy describing the intentions and direction in terms of information security related to aviation safety,
  - the information security objectives set to implement this strategy,
  - the steps and action plan to achieve these objectives.

3.2.2. Coherence between strategy and objectives

IS.I/D.OR 200 a) 1)

The Accountable Manager ensures coherence between:

- the information security strategy and objectives and,
- the overall strategy and objectives of the organisation and those specific to aviation safety.

3.2.3. Integration or interaction between management systems

IS.I/D.OR 200 d)

The Accountable Manager specifies the integration or interaction between the ISMS and existing management systems in the organisation. Specifically:

- the Aviation Safety Management System (SMS),
- if applicable, other Information Security Management Systems interacting with the aviation ISMS, such as a shared ISMS within a group of companies meeting other regulatory, internal, and/or economic objectives.

3.2.4. Communication of the information security policy

IS.I/D.OR 240 a) 2)

The Accountable Manager ensures that the information security policy is:

- appropriately disseminated and promoted:
  - within the organisation,
  - to partners including subcontractors, service providers, and equipment suppliers.
- formalized and integrated or referenced in:
  - the information security management system manual or,
  - the safety management system manual of the organisation.

3.3. Resource management, roles, and responsibilities

IS.I/D.OR 240 a) 1) and 3)
IS.I/D.OR 240 b), c), e) and f)

The Accountable Manager:
- is able to demonstrate knowledge of Part-IS regulation,
- ensures that the financial, material, and human resources necessary for managing information security risks related to aviation safety are available and sufficient,
- defines and assigns roles and responsibilities for managing information security related to aviation safety.

Specifically, the Accountable Manager:
- appoints a person or group of persons responsible for:
  - implementing Part-IS regulation, ensuring they have:
    - direct access to the Accountable Manager,
    - sufficient authority and competencies to perform their functions,
    - provision for interim arrangements in case of absence.
  - ensuring compliance with Part-IS regulation.
- formalizes the designation of these individuals or groups specifying:
  - their titles, names, missions,
  - their direct link with the Accountable Manager, their responsibilities, powers, and resources through an organisational chart,
  - their reporting obligations,
- ensures that roles and responsibilities are communicated and known at all levels of the organisation, both internally and with relevant external partners.

The elements related to resource management, roles, and responsibilities are:
- formalized,
- integrated or referenced in:
  - the information security management system manual or,
  - the safety management system manual of the organisation.

IS.I/D.OR 240 d) and e)

Where the organisation shares information security organisational structures, policies, processes and procedures with other organisations or with areas of their own organisation which are not part of the approval or declaration, the Accountable Manager may delegate its activities to a common responsible person.

In such a case:
- the common responsible person:
  - is formally appointed,
  - has direct access to the accountable manager,
  - is able to demonstrate knowledge of the Part-IS Regulation,
  - defines and approves the information security policy,
  - designates a person or group of people responsible for implementing the Part- Is Regulation, who:
    - have direct access to the common responsible person,
    - possess sufficient authority and competencies to perform their functions,
    - are covered by interim arrangements in case of absence.
- the accountable manager:
  - formally designates the common responsible person,
  - endorses the common responsible person policy and undertakes to enforce it within their scope.
- the common responsible person and the accountable manager:
  - define and are able to demonstrate their knowledge of the scope of responsibility and the limits of the implemented organisation,
  - proactively manage issues,
  - document and address any warning signs of non-compliance.

4. Information security risk management

IS.I/D.OR 205 c) *Regulation (UE) n°2015/1998-1.7.1, 1.7.2 and 1.7.3*

As part of information security risk management activities related to aviation safety and/or security, the organisation:

- defines the responsibilities of various internal and external participants,
- specifies the interaction with the existing organisation for managing risks related to aviation safety and/or security,
- details the methodology or standard used to carry out these activities or provides evidence that it:
  - produces:
    - reproducible results based on similar input elements,
    - results that are comparable over time,
  - considers relevant and valid input elements,
  - allows iterative refinement of results over time and available input elements.
- formalizes procedures related to risk management, particularly
  - risk assessment and treatment,
  - information security incident management,
  - management of interfacing organisations,
  - management of subcontractors performing ISMS activities.
- integrates or refers to these procedures in:
  - the information security management system manual or,
  - the safety management system manual of the organisation and/or,
  - the security program.

For subsequent activities, the organisation relies on its chosen risk management methodology to reach conclusions. However, the different steps and expected documents for regulatory compliance are specified below.

➔ Best practice #1: Methodology and standard for information security risk management

4.1. Establishing the context

IS.I/D.OR 205 a) 1) *Regulation (UE) n°2015/1998-1.7.1, 1.7.2 and 1.7.3*

To define the scope of its risk assessment and/or its ISMS, the organisation identifies the list of functions related to its security missions and/or aviation safety.

To achieve this, it may rely on the lists of functions in appendix II and appendix III.

Additionally, the organisation defines scales for:

- the severity of consequences in terms of security and/or aviation safety,
- the probability of occurrence (or likelihood) of the risk,
- the risk acceptance criteria specific to the organisation.

➔ Best practice #2: Defining the scope of information security risk management and ISMS

➔ Best practice #3: Defining scales for information security risk management

4.2. Risk assessment

4.2.1. Risk identification

IS.I/D.OR 205 a) and b) — *Regulation (UE) n°2015/1998-1.7.1, 1.7.2 and 1.7.3*

Based on the list of functions related to the security and/or aviation safety of the organisation, the organisation identifies:

- the functions:
  - for which it is responsible for, and which are performed by itself for its own account and/or,
  - that it implements on behalf of an external partner (interface) and/or,
  - for which it is responsible for, and which are performed by an external partner on behalf of the organisation (interface).
- the elements that contribute to the realization of each of the previously identified functions, including equipment, systems, data, and information.

Then, for each identified function and element, the organisation:

- provides a description,
- identifies one or more responsible persons and/or entities, which may be internal or external,
- specifies, if applicable, whether there is an interface with a third party and the nature of this interface:
  - service provision,
  - subcontracting,
  - supply of equipment,
  - client,
  - partner,
  - other service, to be specified.

The organisation has an interface with another organisation when the realization of a function requires:

- *exchanging data and/or information with that third party,*
- *providing and/or making available a system, equipment, and/or digital service for that third party,*
- *using an information system, equipment, and/or digital service provided by that third party.*

Finally, the organisation:

- determines, for each identified function, alone or in conjunction with the interfacing organisations concerned:
  - the undesirable events, particularly adverse effects on security and/or aviation safety resulting from a breach in availability, integrity, confidentiality, and authenticity of the function,
  - the impacts on security and/or aviation safety associated with these undesirable events.
- formalises the list of interfacing organisations previously identified.

➔ Best practice #4: Determining the cybersecurity baseline and gaps

4.2.2. Risk analysis

IS.I/D.OR 205 c) 1) — *Regulation (UE) n°2015/1998-1.7.1, 1.7.2 and 1.7.3*

Then, the organisation:

- defines a likelihood scale (or probability of occurrence) taking into account:
  - the likelihood of occurrence of the undesirable event at the level of the element(s) of the concerned information system(s),
  - the effectiveness of the security and/or aviation safety business processes in place within the organisation that can block, limit, or foster the occurrence of the undesirable event. For example, the protection barriers already implemented against the undesirable event.
- identifies its risks based on the impact analysis by associating with the undesirable events:
  - a severity level according to the predefined scale,
  - a likelihood level according to the predefined scale,
- one or more responsible persons and/or entities, which can be within the organisation or an external partner, especially for the incoming functions.

IS.I/D.OR 205 e)

Only for organisations addressed by the Part-ATM/ANS: Organisations required to comply with Subpart C of Annex III (Part-ATM/ANS.OR) to Implementing Regulation (EU) 2017/373 shall replace the risk with an impact analysis on their services as per the safety support assessment required by point ATM/ANS.OR.C.005.

4.2.3.Risk evaluation

IS.I/D.OR 205 c) 1) *Regulation (UE) n°2015/1998-1.7.1, 1.7.2 and 1.7.3*

Finally, the organisation:
- associates each identified risk with its risk level according to the predefined scale based on:
  - the results of its risk analysis,
  - the risk analysis information provided as part of a function performed by a third party.
- formalises the list of interfacing organisations that present a risk to security and/or aviation safety.

4.2.4.Risk assessment outcome

IS.I/D.OR 205 c) 2) *Regulation (UE) n°2015/1998-1.7.1, 1.7.2 and 1.7.3*
IS.I/D.OR 210 b) *AIM-DR-1-7-1-(I)*

The organisation:
- formalizes:
  - the list of risks related to security and/or aviation safety, specifying for each:
    - the associated function and any potential interfaces,
    - the equipment, systems, data, and information that contribute to the realization of the associated function, as well as any potential interfaces,
    - the associated undesirable event,
    - one or more responsible persons and/or entities,
    - the risk levels.
  - the list of interfacing organisations presenting a risk to security and/or aviation safety,
  - if applicable, the list of critical information systems regarding security.
- has the list of risks related to aviation security and/or safety approved by its Accountable Manager and as applicable, by the person(s) or entities responsible for the risks, in accordance with the organisation risk management structure,
- retains documented information as evidence of the risk assessment outcomes.

IS.I/D.OR 205 e)

Only for organisations addressed by the Part-ATM/ANS: Organisations required to comply with Subpart C of Annex III (Part-ATM/ANS.OR) to Implementing Regulation (EU) 2017/373 shall make the safety support assessment available to the air traffic service providers to whom they provide services.

Those air traffic service providers shall be responsible for evaluating the impact on aviation safety.

4.3. Risk treatment

4.3.1. Measures for risk treatment

IS.I/D.OR 210 a) *Regulation (UE) n°2015/1998-1.7.1, 1.7.2 and 1.7.3*

Based on the results of the risk assessment, the organisation:
- defines and justifies for each risk related to security and/or aviation safety whether to:
  - maintain the risk if it is acceptable as is,
  - reduce the risk level by introducing, removing, or modifying information security measures,
  - avoid the risk by discontinuing the activity or situation that gives rise to the risk,
  - share the risk with another party capable of managing the risk more effectively.
- determines the measures to treat the risk according to the chosen action, ensuring they do not introduce new risks,
- implements and verifies the effectiveness of these measures in a timely manner in accordance with §6.1 and §6.2.3.

4.3.2. Development of the risk treatment plan

IS.I/D.OR 210 a) *Regulation (UE) n°2015/1998-1.7.1, 1.7.2 and 1.7.3*

The organisation develops a risk treatment plan for security and/or aviation safety, identifying for each determined information security measure:
- the addressed risk,
- the person(s) responsible for implementing the information security measure,
- The priority of implementation,
- The recommended implementation timeframe,
- Reasons preventing implementation, if any.

4.3.3. Evaluation of residual risks

IS.I/D.OR 210 a) *Regulation (UE) n°2015/1998-1.7.1, 1.7.2 and 1.7.3*

The organisation evaluates residual risks after applying the information security measures defined in the risk treatment plan. If a residual risk remains unacceptable, the organisation re-treats it in accordance with §4.3.1, until it is acceptable.

4.3.4. Risk Treatment Outcomes

IS.I/D.OR 210 b) *Regulation (UE) n°2015/1998-1.7.1, 1.7.2 and 1.7.3*

The organisation:
- formalizes:
  - the risk treatment plan for security and/or aviation safety,
  - the list of residual risks after applying the risk treatment plan for security and/or aviation safety.
- has these documents approved by the Accountable Manager and/or the responsible person(s) and/or entities according to its risk management organisation,
- retains documented information as evidence of the risk assessment outcomes.

4.4. Information security incident management

IS.I/D.OR 200 a) 5) *Regulation (UE) n°2015/1998-1.7.2*

The organisation defines, implements and formalizes technical and organisational measures aimed at:
- detecting information security incidents and identifying those having a potential impact on security and/or aviation safety,
- responding to detected information security incidents with a potential impact on security and/or aviation safety,
- recovering from information security incidents having a potential impact on security and/or aviation safety.

➔ Best practice #5: Information security incident management measures

4.4.1. Detection of information security incidents

4.4.1.1. Identification of undesirable information security incidents

IS.I/D.OR 220 a)

The organisation identifies the list of types of undesirable information security incidents with a potential impact on aviation safety, along with the associated impacts and consequences, based on the results of the risk assessment and treatment conducted in §4.2. and §4.3.

➔ Best practice #6: Identification of undesirable information security incidents

4.4.1.2. Sources for the collection of events

4.4.1.2.1. Sources for the automatic collection of events

IS.I/D.OR 220 a)

Based on the undesirable information security incidents with a potential impact on aviation safety, the organisation:
- identifies relevant collection sources within its information system,
- monitors vulnerabilities that may affect its information system,
- logs relevant events for detection among the identified collection sources and vulnerability monitoring.

➔ Best practice #7: Automatic collection sources for information security events

4.4.1.2.2. Internal event reporting

IS.I/D.OR 215 a), b) 1) and e)

The organisation implements an internal reporting system for information security events having a potential impact on aviation safety. This system:
- identifies the events that must be reported, namely information security events with potential impact on aviation safety,
- specifies the means made available to report an event as well as the deadlines,
- is accessible to individuals who need to know among:
  - Its internal personnel,
  - Relevant third parties in the context, identified in §4.2.1,
  - All relevant stakeholders.

The organisation:
  - may integrate this internal event reporting system into an existing system,
  - formalizes the description of this system and integrates it or refers to it in:
    - The information security management system manual, or,
    - The safety management system manual of the organisation.

4.4.1.3. Events detection strategy

IS.I/D.OR 215 b) 3)

The organisation implements a strategy for detecting information security events having a potential impact on aviation safety. This strategy:

- defines, based on the risk assessment, a classification by severity order of information security incidents having a potential impact on aviation safety,
- defines detection rules based on:
  - the collection sources previously defined,
  - the list of undesirable information security incidents identified previously,
  - internal and external knowledge basis.
- defines rules for the conservation of events that specify:
  - conservation criteria,
  - conservation duration,
  - revaluation frequency,
  - deletion criteria.
- ensures the centralization and correlation of events,
- allows identification of deviations from the predetermined references values related to functional performance.

➔ Best practice #8: Defining information security events detection rules

4.4.1.4. Evaluation and Qualification of information security incidents and vulnerabilities

IS.I/D.OR 215 b) 2)

The organisation implements an evaluation and qualification procedure of detected events having a potential impact on aviation safety. This procedure:

- identifies the scope of the detected event,
- assesses the impacts and severity in relation to aviation safety,
- determines the causes of the detected event,
- identifies any internal and/or external stakeholders affected by the detected event,
- evaluates if the detected event qualifies as an incident or a vulnerability.

4.4.1.5. Information security notification

IS.I/D.OR 215 b) 4)
IS.I/D.OR 220 a) 2)
IS.I/D.OR 230 b) and c) 1)

As soon as event is classified as a security incident, the organisation notifies:

- the relevant individuals within its organisation to activate appropriate reactions,
- the competent authority according to the framework defined in §4.4.4,
- if required, the external partners concerned according to the framework defined in §4.5.1.

4.4.2.Information security incident response

IS.I/D.OR 220 b)

The organisation defines an incident response mechanism that:

- specifies:
  - the roles and responsibilities of individuals who activate responses in the event of a qualified incident,
  - the methods for informing these individuals, including tools and timelines.
- defines immediate actions to be implemented and associated timelines by identifying:
  - the resources to be activated within and outside the organisation,
- the organisational and technical measures that can be implemented to limit the spread of an attack and prevent the occurrence of undesirable incidents.

➔ Best practice #9: Defining immediate actions to respond to an information security incident

4.4.3.Recovery

IS.I/D.OR 220 c)

The organisation defines a recovery procedure following an information security incident, which:
- specifies the roles and responsibilities of individuals managing recovery actions,
- defines how to identify the scope of the impacted information system,
- defines the recovery actions to be implemented to return to a safe state and specifies:
  - priorities,
  - resources to be activated.
- determines the objectives of time to return to service according to the severity, the nature and the context of the incident.

➔ Best practice #10: Defining recovery actions following a security incident

4.4.4.Notification to the competent authority

IS.I/D.OR 230 a), b) and c)

When an information security event is qualified as an information security incident or vulnerability having a potential significant impact on aviation safety, then the incident or vulnerability has to be considered as an aviation safety event.

Thus, the organisation articulates its information security risk management with the external reporting mechanism set up within the framework of its SGS or its navigability monitoring process.

When the required elements for the notification and those present in the following reports are sensitives for the organisation, then the organisation communicates:
- only non-sensitive elements via ECCAIRS2,
- the most sensitive elements through distinct secure channels, referencing the notification in ECCAIRS2.

➔ Best practice #11: Secure transmission of sensitive information for notification to the competent authority

4.5. Third-party risk management

4.5.1. Interfacing organisations

4.5.1.1. Organisations posing a risk to aviation security.

AIM-B-2
AIM-B-4

Based on the list of interfacing organisations posing a risk to aviation security as identified in §4.2, the organisation implements a framework with these entities that:

- sets information exchange rules to ensure the authenticity, confidentiality, and integrity of the exchanged information, as well as the anonymity of interlocutors if desired,
- specifies requirements to be applied, which include:
  - regulatory, such as:
    - background checks,
    - information security awareness and training.
  - contractual, such as:
    - implementing information security measures defined by the organisation,
    - monitoring adapted to the context of third-party activities.
- The organisation retains documented information as evidence of managing interfacing organisations posing a risk to aviation security.

4.5.1.2. Organisations posing a risk to aviation safety.

4.5.1.2.1. Interfacing organisations with safety approval or certification

IS.I/D.OR 200 a) 13)
IS.I/D.OR 215 c) and d)

Based on the list of interfacing organisations posing a risk to aviation safety as identified in §4.2.4, the organisation:

- identifies third parties posing a risk to aviation safety that must comply with Part-IS regulations, known as contractors,
- implements a framework with these entities that includes:
  - defining responsibilities for managing shared risks,
  - sharing safety assumptions and objectives for relevant scopes,
  - reporting information security events having a potential significant impact on aviation safety in accordance with §4.4.1.2.2,
  - information exchange rules to ensure the authenticity, confidentiality, and integrity of the exchanged information, as well as the anonymity of interlocutors if desired.

The organisation retains documented information as evidence of managing approved or certified interfacing organisations posing a risk to aviation safety.

IS.I/D.OR 230 a), b) and c)

When the organisation has an interface with an organisation that holds a design approval or that is responsible for the design of a system or component, then it integrates in its working framework:

- notification of information security incidents or vulnerabilities having a significant impact on aviation safety:
  - to the holder of the design approval when an aircraft or an associated system or element is affected,
  - to the system or component design owner a when a system or component used by the organisation is affected.
- Submission of a report:
  - to the holder of design approval or to the organisation responsible for the design of the system or component,
  - as soon as possible, but without exceeding 72 hours from the time the organisation became aware of the situation, unless exceptional circumstances prevent it.
- Submission of a follow -up report:
  - to the holder of design approval or to the organisation responsible for the design of the system or component,
  - specifying the measures that the organisation:
    - has taken or intends to take to recover from the incident and,
    - intends to take to prevent such information security incidents in the future.

4.5.1.2.2. Interfacing organisations without safety approval or certification

IS.I/D.OR 200 a) 13)
IS.I/D.OR 215 c) and d)

Based on the list of interfacing organisations posing a risk to aviation safety as identified in §4.2.4, the organisation:
- identifies third parties posing a risk to aviation safety that are not required to comply with Part-IS regulations,
- defines:
  - when possible, a framework with these entities that includes:
    - reporting of information security events and vulnerabilities having a potential significant impact on aviation safety in accordance with §4.4.1.2.2,
    - information exchange rules to ensure the authenticity, confidentiality, and integrity of the exchanged information, as well as the anonymity of interlocutors if desired,
    - implementing information security measures defined by the organisation and monitoring adapted to the context of third-party activities,
    - if applicable, personnel reliability checks according to the organisation's reliability control policy (§5.2).
  - otherwise, the organisation manages this risk within the framework of §4.3.

The organisation retains documented information as evidence of managing non-approved or non-certified interfacing organisations posing a risk to aviation safety.

➔ Best practice #12: Technical references for third party management

4.5.2.Subcontracting of ISMS activities

IS.I/D.OR 235 a) and b)

The organisation identifies subcontractors involved in one or more activities of its ISMS. These include third parties participating in:
- risk management (assessment, risk treatment, and incident management),
- ISMS operations.

When the organisation uses subcontracting in this context, the organisation:
- conducts a risk assessment related to the contracting of one or more of these activities based on an assessment of:
  - the subcontractor's competencies,
  - the subcontractor's experience for the concerned activities,
  - the subcontractor's economic and technical reliability,
- develops a contract specifying:
  - the organisation of the service:
    - roles and responsibilities between the organisation and the subcontractor,
    - a clear reporting structure between the organisation and the subcontractor,
    - the method and tools for service monitoring,
  - the service scope,
  - applicable requirements for the concerned ISMS activities,
  - management of access authorizations to the organisation's information,
  - confidentiality clauses,
  - possible actions in case of contract breach,
  - the possibility for the organisation to conduct audits,
  - the competent authority's access to the subcontractor,
  - notification to the organisation of information security events and vulnerabilities having a potential significant impact on aviation safety in accordance with §4.4.1.2.2.

Finally, the organisation:
- formalizes the list of subcontractors involved in one or more activities of its ISMS,
- retains documented information as evidence of the management of subcontractors for ISMS activities.

➔ Best practice #13: Subcontracting of ISMS activities

5. Personnel and competencies

5.1. Background checks and trustworthiness control

5.1.1. Background checks for aviation security personnel

5.1.1.1. Aviation security personnel

Regulation (UE) n°2015/1998-11.1.2 c)

Based on its risk assessment, the organisation identifies or has identified by third parties specified in §4.2, the individuals who:

- have administrator rights or unsupervised and unlimited access to critical information and communication technology data and systems used for aviation security, identified in§4.2., and/or,
- have been identified during the aviation security risk assessment in §4.2.

This includes:

- management teams, *i.e.*, individuals organizing, directing, controlling, or participating in the management of information security risks affecting aviation security (CISO, CIO, internal auditor, security manager, etc.),
- operational teams, i.e., individuals defining, planning, and implementing the information security measures defined in §4.3 on critical information systems identified in §4.2,
- administrators of critical information systems identified in §4.2,
- users with unsupervised and unlimited access to critical information systems identified in §4.2,
- if applicable, individuals and/or entities responsible for aviation security risks identified in§4.2.

The organisation retains appropriate documented information as evidence of the identification of aviation security personnel.

5.1.1.2. Enhanced background checks for aviation security personnel

Regulation (UE) n°2015/1998-11.1.2 c), 11.1.3 and 11.1.7
Code of transports: L 6342-3, R 6342-32 and R 6342-33

The organisation applies or has applied by third parties identified in §4.2, enhanced background checks for previously identified aviation security personnel. The organisation ensures the following actions are implemented, or ensures their implementation by third parties:

- ensures these individuals have a prefectural authorization as required by Article L6342-3 of the Transport Code, namely:
  - they have a valid access badge to a regulated security zone, which requires the prefectural authorization, or,
  - they have a valid authorization without a badge.
- considers the employment, education, and any interruptions in the states where these individuals have resided over the past 5 years,
- renews these checks at regular intervals not exceeding 12 months,
- pays particular attention to any unexplained interruptions, requesting explanations or justifications and documenting that this verification has been completed.

The organisation:

- maintains an updated list of security personnel who have undergone identity verification and hold a valid authorization,
- formalizes its background check procedure for security personnel,
- integrates or refers to this procedure in the security program,
- retains appropriate documented information as evidence of the background checks.

5.1.2. Trustworthiness control of aviation safety personnel

IS.I/D.OR 240 i)

Based on its risk assessment, the organisation defines its policy for controlling the trustworthiness of individuals, where the control on each person is proportional to the impact that they could have on aviation safety by compromising the integrity, confidentiality, authenticity or availability of data.

This policy identifies:

- categories of individuals based on their risk to aviation safety,
- trustworthiness control measures that:
  - establish at minimum the person's identity through the verification of an identity document,
  - may, depending on the previously identified categories and their level of risk to aviation safety:
    - consider the employment, education, and any interruptions[3] of these individuals in the states where they have resided[4] over the past 5 years,
    - lead to a background check of these individuals.

The organisation:

- applies or has applied by third parties identified in §4.2, the policy for controlling the trustworthiness of individuals,
- maintains an updated list of aviation safety personnel who have undergone identity verification and trustworthiness control, specifying the type based on their risk to aviation safety,
- formalizes the policy for controlling personnel trustworthiness,
- integrates or refers to this policy in:
  - the information security management system manual, or,
  - the safety management system manual of the organisation,
- retains appropriate documented information as evidence of personnel trustworthiness control:
  - as long as the personnel concerned are subject to a background check, and,
  - for one year after the end of the activity justifying the trustworthiness control.

➔ Best practice #14: Background check for trustworthiness controls

5.1.3. Special cases

5.1.3.1. Personnel subject to security and safety requirements

Regulation (UE) n°2015/1998-11.1.2 c), 11.1.3 and 11.1.7
Code of transports: L 6342-3, R 6342-32 and R 6342-33

IS.I/D.OR 240 i)

When an individual is subject to background check requirements for both security and aviation safety, they must comply with the most stringent requirements, which are those for security

5.1.3.2. Personnel abroad

Regulation (UE) n°2015/1998-11.1.2 c), 11.1.3 and 11.1.7
Code of transports: L 6342-3, R 6342-32 and R 6342-33

IS.I/D.OR 240 i)

If the organisation employs foreign nationals residing outside of France and it has been demonstrated that it is not possible to perform a background check, then the organisation requires:

- an official identity document of the employee to verify their identity, and,
- when background check is required:
  - a document equivalent to a criminal record extract for countries able to provide this type of document,
  - or in the absence of a similar document, a commitment signed by the employee, of good conduct when carrying out missions on behalf of the organisation.

The organisation:

- keeps up to date a list of foreign employees for whom the background check could not be carried out,
- precises for each employee the actions implemented to ensure their trustworthiness.

Note: Subject to applicable laws, some countries may provide, at the request of the employer, an extract from the criminal record (e.g. India, Morocco). The extract from the criminal record provided can be similar, or even more provided than a French criminal record. The demand is facilitated when the employer is settled in this country.

[3] "Interruption": Any interruption of more than 28 days in the statement of the initial training or the career.
[4] "State of residence": any country in which the person has been constantly residing for 6 months or more.

5.2. Awareness

Regulation (UE) n°2015/1998-11.2.1.4, 11.2.8.1 and 11.2.8.2
AIM 11-2-1-4 and 11-2-1-5

IS.I/D.OR 240 h)

The organisation implements an awareness campaign or ensures its implementation by the third parties identified in §4.2 specifically, by:

- specifying:
  - the means and resources deployed,
  - the frequency of the awareness campaign renewal.
- ensuring that the individuals identified in §5.1.1.1. and through the aviation safety risk assessment (§4.2) are made aware of information security,
- formalizing the monitoring of the awareness and the associated procedure,
- integrating or refers to this procedure in:
  - the information security management system manual, or,
  - the safety management system manual of the organisation, and/or,
  - the security program.
- retaining appropriate documented information as evidence of monitoring personnel awareness.

➔ Best practice #15: Designing cybersecurity awareness training

5.3. Training

Regulation (UE) n°2015/1998-11.2.1.4, 11.2.8.1 and 11.2.8.2
AIM 11-2-1-4 and 11-2-1-5

IS.I/D.OR 240 g)

The organisation implements a training program or ensures its implementation by the third parties identified in §4.2, specifically by:

- identifying the needs within the company, ensuring that:
  - management teams are trained in information security management in line with their assigned tasks,
  - operational teams are trained in the implementation of state-of-the-art information security measures in line with their assigned tasks.
- specifying the means and resources deployed,
- formalizing the monitoring of competencies and the associated procedure,
- integrating or referencing this procedure in:
  - the information security management system manual, or,
  - the safety management system manual of the organisation, and/or,
  - the security program.
- retaining appropriate documented information as evidence of personnel training monitoring.

➔ Best practice #16: Designing cybersecurity training

6. Definition and operation of the ISMS

6.1. Information security risk management monitoring

6.1.1. Organisation of information security risk management monitoring

IS.I/D.OR 200 a) 2) to 6) and 8) to 10)
IS.I/D.OR 205 d)
Regulation (UE) n°2015/1998-1.7.1, 1.7.2 and 1.7.3
AIM-DR 1-7-1 (II)

The organisation defines the internal mechanism for monitoring risk management and specifies:
- the structure and positioning,
- the responsibilities of different participants,
- the interaction even integration with the existing organisation for monitoring risk management related to security and/or aviation safety,
- the periodicity and/or significant events that activate this mechanism, particularly when:
  - there is a change in elements exposed to information security risks,
  - there is a change in interfaces between the organisation and other entities, or in risks communicated by other entities,
  - there is a change in information or knowledge used for identifying, analysing, and classifying risks,
  - analysis of information security incidents has provided new insights.

6.1.2. Missions of risk management monitoring

IS.I/D.OR 200 a) 2) to 6) and 8) to 10)
IS.I/D.OR 205 d)
Regulation (UE) n°2015/1998-1.7.1, 1.7.2 and 1.7.3
AIM-DR 1-7-1 (II) and B-3

Periodically and/or during significant events, the organisation:
- plans, implements, and controls:
  - risk management activities:
    - risk assessment (§4.2),
    - risk treatment (§4.3),
    - information security incident management (§4.4),
    - management of risks induced by third parties (§4.5),
  - management of personnel and competencies (§5),
  - implementation of technical and organisational measures:
    - from the risk treatment plan,
    - for detection, reaction, and response to a security incident,
    - notified by the competent authority.
- ensures the monitoring of information security events and incidents.

6.1.3. Outcome of risk management monitoring

IS.I/D.OR 200 a) 2) to 6) and 8) to 10)
IS.I/D.OR 205 d)
Regulation (UE) n°2015/1998-1.7.1, 1.7.2 and 1.7.3
AIM-DR 1-7-1 (II)

The organisation:
- produces and maintains dashboards for monitoring:
  - risk management activities,
  - personnel and competencies,
  - progress in implementing technical and organisational measures,
  - information security events and incidents,
- informs the Accountable Manager and individuals or entities responsible for risks of the conclusions of risk management monitoring,
- formalizes the procedure for risk management monitoring,
- integrates or refers to this procedure in:
  - the information security management system manual, or
  - the safety management system manual of the organisation, and/or
  - the security program,
- retains documented information as evidence of risk management monitoring.

6.2. Evaluation of the ISMS

6.2.1. Evaluation of ISMS compliance

6.2.1.1. Organisation of ISMS compliance evaluation

IS.I/D.OR 200 a) 12)

The organisation defines the internal mechanism responsible for compliance evaluation and specifies:
- the structure and positioning,
- the responsibilities of different participants, ensuring that evaluators are independent from those responsible for ISMS implementation.,
- the interaction even integration with the existing organisation for compliance evaluation related to aviation safety,
- the periodicity and/or significant events that activate this mechanism.

6.2.1.2. Missions of ISMS compliance evaluation

IS.I/D.OR 200 a) 12)

Periodically and/or during significant events, and based on the results of:
- internal audits,
- audits by competent authorities.

the organisation:
- evaluates compliance,
- identifies discrepancies in its ISMS with respect to the provisions of this document,
- corrects these discrepancies to comply with Part-IS requirements.

6.2.1.3. Outcome of ISMS compliance evaluation

IS.I/D.OR 200 a) 12)

The organisation:
- produces and maintains a compliance monitoring dashboard and any associated discrepancies,
- informs the Accountable Manager and individuals or entities responsible for risks of the conclusions of the ISMS compliance evaluation,
- formalizes the procedure for ISMS compliance evaluation,
- integrates or refers to this procedure in:
  - the information security management system manual, or
  - the safety management system manual of the organisation.
- retains documented information as evidence of the outcomes of the ISMS compliance evaluation.

6.2.2. Response to findings notified by the competent authority

IS.I/D.OR 200 a) 7)
IS.I/D.OR 225 a) and b)

The organisation responds to findings notified by the competent authority through the finding treatment process provided within its certificate/approval scope.

6.2.3.Evaluation of ISMS effectiveness and maturity

6.2.3.1. Organisation of ISMS effectiveness and maturity evaluation

IS.I/D.OR 260 a)

The organisation defines the internal mechanism responsible for evaluating the effectiveness and maturity of the ISMS and specifies:

- the structure and positioning,
- the responsibilities of different participants,
- the interaction even the integration with the existing organisation for evaluating the aviation safety management system,
- the periodicity and/or significant events that activate this mechanism,
- the effectiveness indicators associated with the safety objectives defined in the information security policy,
- the targeted ISMS maturity model.

➔ Best practice #17: ISMS maturity models

6.2.3.2. Missions of ISMS effectiveness and maturity evaluation

IS.I/D.OR 260 a)

Periodically and/or during significant events, and based on:

- the information security policy,
- elements related to resource management, roles, and responsibilities,
- monitoring dashboards for risk management activities, personnel and competencies, and information security events and incidents,
- potential technical and organisational audits,
- experience feedback, particularly from incident management.

the organisation:

- evaluates:
  - the effectiveness of its ISMS against the safety objectives defined in the information security policy,
  - the maturity of its ISMS against the targeted maturity model. During these evaluations, the organisation pays particular attention to processes related to:
    - governance (§3),
    - risk management activities (§4) and their monitoring (§6.1),
    - personnel and competency management (§5),
    - evaluation of compliance, effectiveness, and maturity of the ISMS (§6.2),
    - continuous improvement management (§6.3).
- identifies:
  - discrepancies and/or gaps relative to safety objectives,
  - potential areas for improvement to achieve the targeted maturity levels.

6.2.3.3. Outcome of SMS effectiveness and maturity evaluation

IS.I/D.OR 260 a)

The organisation:

- produces and maintains dashboards for monitoring:
  - the effectiveness of its ISMS and associated discrepancies,
  - the maturity of its ISMS and any associated areas for improvement,
- informs the Accountable Manager and individuals or entities responsible for risks of the conclusions of the ISMS effectiveness and maturity evaluation,
- formalizes the procedure for ISMS effectiveness and maturity evaluation,
- integrates or refers to this procedure in:
  - the information security management system manual, or
  - the safety management system manual of the organisation,
- retains documented information as evidence of the outcomes of the ISMS effectiveness and maturity evaluation.

6.3. Continuous improvement of the ISMS

6.3.1. Organisation of ISMS continuous improvement management

IS.I/D.OR 200 b)
IS.I/D.OR 260 b)

The organisation defines the mechanism for managing continuous improvement and specifies:
- the structure and positioning,
- the responsibilities of different participants,
- the interaction even the integration with the existing organisation for managing continuous improvement of the aviation safety management system,
- the periodicity and/or significant events that activate this mechanism, particularly:
    - the frequency between two audits of the competent authority, and/or,
    - significant events triggering management review (incident, context change, etc.).

6.3.2. Missions of ISMS continuous improvement management

IS.I/D.OR 200 b)
IS.I/D.OR 260 b)

Periodically and/or during significant events and based on:
- changes in the organisation's context, particularly:
    - the evolution of threats,
    - changes in the organisation.
- monitoring dashboards:
    - ISMS compliance and associated discrepancies,
    - ISMS effectiveness and associated discrepancies,
    - ISMS maturity and potential areas for improvement,
    - non-conformities notified by the competent authority and associated corrective actions,
    - actions from continuous improvement management.

the organisation:
- identifies:
    - modifications to the ISMS: organisation, processes, etc.,
    - corrective and preventive actions to be implemented,
    - opportunities for continuous improvement.
- decides to implement them,
- specifies the implementation timelines.

6.3.3. Conclusions on the ISMS Continuous Improvement Management

IS.I/D.OR 200 b)
IS.I/D.OR 260 b)

The organisation:
- produces and maintains a dashboard for tracking actions resulting from the continuous improvement management,
- formalizes the procedure related to continuous improvement,
- integrates or refers to this procedure in:
    - the information security management system manual, or
    - the safety management system manual of the organisation,
- retains documented information as evidence of the continuous improvement management.

6.4. Changes to the information security management system

IS.I/D.OR 200 c)
IS.I/D.OR 250 c)
IS.I/D.OR 255 a)

The organisation defines a “Management of ISMS changes not subject to approval” procedure. This procedure:

- is approved by the competent authority,
- specifies the method for classifying changes between those “subject to prior approval” and those “subject to notification”,
- includes the assessment of a “cybersecurity” risk analysis for any ISMS changes,
- includes the following changes:
    - changes to “cybersecurity” risk analysis method for any ISMS changes,
    - changes to the event notification process,
    - amendments to the ISMS manual (excluding those subjects to approval).

The organisation may integrate this procedure into the existing SMS change management procedure.

IS.I/D.OR 200 c)
IS.I/D.OR 250 c)
IS.I/D.OR 255 b)

Following changes are subjected to approval by the competent authority:

- Major changes to the chain of responsibility within the ISMS, including:
    - the ISMS manager,
    - the ISMS compliance manager,
    - if applicable, the common responsible person.
- Major changes to the information security policy with a potential impact on aviation safety,
- Major changes relating to the "Management of ISMS changes not subject to approval" procedure.

The organisation integrates or refers to these changes, which are subject to approval by the competent authority in:

- the information security management system manual, or,
- the safety management system manual of the organisation.

7. Record keeping

7.1. Procedure of record keeping

IS.I/D.OR 200 a)
IS.I/D.OR 245 c) et d)

The organisation:
- updates its procedure of record keeping in order to:
  - integrate the elements specified in §7.2,
  - integrate protection means proportional to the sensitivity of documents and the need for availability,
  - plan for the destruction of these documents and the disposal of storage media when archiving is no longer necessary. The security of destruction and disposal is proportional to the sensitivity of documents and content of the storage media concerned.
- integrates the management of these documents in the scope of its ISMS,
- integrates or refers to this procedure in:
  - the information security management system manual, or,
  - the safety management system manual of the organisation.

7.2. Records to keep

IS.I/D.OR 200 a) 11)
IS.I/D.OR 245 a) et b)

Documents	Retention period
Any approval or certificate issued by the competent authority	At least 5 years after the end of the certificate's/approval's validity
Any dispensation authorization issued by the competent authority including the associated dispensation form	At least 5 years after the end of the dispensation authorization validity
Any contracts relating to the subcontracting of ISMS activities	At least 5 years after the change of the contract or the end of the contract
Any documents relating to key information security risk management processes: - Risk assessment, risk treatment and risk management monitoring - Information security incident management - Third-party risk management - Personnel and competencies management - ISMS evaluation	At least 5 years after the creation of the document
Any documents relating to risk assessment: - Severity and likelihood (or occurrence) scales, - Risk acceptance criteria, - List of information security risks related to aviation safety and associated information, - List of interfacing organisations posing a risk to aviation safety.	At least 5 years after the creation of the document
Any documents relating to risk treatment: - Risk treatment plan, - List of residual risk after application of the risk treatment plan.	At least 5 years after the creation of the document
Any documents relating to internal reporting of information security events and vulnerabilities	At least 5 years after the creation of the document
Any documents relating to external reporting	At least 5 years after the creation of the document
Any documents relating to information security events that may need to be reassessed to reveal undetected information security incident or vulnerabilities.	The retention period is specified in the incident management procedure (§4.4.1.3)
Any documents relating to personnel's information security qualification and experience.	As long as the person works for the organisation AND at least 3 years after the person has left the organisation.

8. Documentation

8.1. Security program

Regulation (UE) n°2015/1998-1.7.1, 1.7.2 and 1.7.3

The organisation integrates or refers to the following elements in its security program:

Documents	3CFv3 Chapters
List of risks affecting security	4.2
List of critical information systems for security	4.2
Risk treatment plan	4.3
List of interfacing organisations posing an information security risk to aviation security	4.2
List of technical and organisational measures to detect, respond, and recover from an information security incident	4.4.4
All documents relating to key processes, procedures, roles and responsibilities implemented to comply with Regulation (EU) n°2015/1998 [1]	

➔ Best practice #18: Examples of elements or references in the security program

8.2. ISMS manual

IS.I/D.OR 250 a) and d)

The organisation integrates or refers to the following elements in:
- the information security management system manual, or,
- the safety management system manual of the organisation.

Documents	3CFv3 Chapters
Commitment letter from the Accountable Manager	3.1
Information security policy	3.2
Titles, names, roles, reporting obligations, responsibilities, and powers of individuals specified in 3.3	3.3
Organisational chart showing hierarchical reporting and responsibilities among individuals specified in 3.3	
General description of human resources in terms of numbers and categories, and the system in place for personnel planning	
Description of the internal notification scheme	4.4.1.2.2
Subcontractor management procedure for ISMS activities	4.5.2
Management of ISMS changes not subject to approval procedure	6.4
All documents relating to key processes, procedures, roles and responsibilities implemented to comply with Part-IS regulation [2,3]	

➔ Best practice #19: Examples of elements or references in the ISMS or SMS manual of the organisation

Appendix

Appendix I: Best practices

Best practice #1: Methodology and standard for information security risk management

When managing information security risks, the organization is advised to use a recognized methodology or standard to carry out risk management activities. This way, the organization will not be required to demonstrate compliance with the methodology or standard used. Below is a non-exhaustive list of recognized methodologies or standards:

- EBIOS Risk Manager: This method, developed by ANSSI, is often used in the French ecosystem and allows for coordination with risk analysis methods derived from aviation safety:
  - EBIOS Risk Manager Guides, ANSSI, Version 1.5, March 2024 [17].
- ISO/IEC 27005: Widely recognized and proven international standard for information security risk management:
  - International Standard ISO/IEC 27005:2022-Information security, cybersecurity, and privacy protection-Recommendations for information security risk management [18].
- ICAO/GCRC risk analysis methodology: Method developed by ICAO and published in the GCRC document enabling the integration of cybersecurity into methods for managing aviation safety, aviation security, or air navigation capacity/efficiency risks:
  - ICAO/GCRC risk analysis methodology [19].
- Any other method compliant with ISO/IEC 31000, the standard for risk management:
  - International standard ISO/IEC 31000:2018-Risk Management-Guidelines [20].

Best practice #2: Defining the scope of information security risk management and ISMS

In order to define the scope of the risk analysis and/or ISMS, the organisation is advised to refer to:

- the lists of functions relating to aviation safety and/or security specified in Appendix II and Appendix III,
- a preliminary risk assessment that identifies the most critical functions to be considered in terms of distance and likelihood of propagation to the aviation safety and/or security impact that is being sought to be prevented:
  - White paper: Identification and Classification guidance for Part-IS assets-ED/DO-ISMS Guidance for Aviation, EUROCAE WG-72 / RTCA SC-216, 2023. [21] The document is available on request.

Best practice #3: Defining scales for information security risk management

In the context of managing information security risks, it is necessary to define different scales that allow results to be compared at each iteration. To achieve this, the organisation is advised to use or draw inspiration from the following reference frameworks:

- EBIOS Risk Manager Guides, ANSSI, Version 1.5, March 2024 [17], page 26,
- ICAO Doc 9859 Safety Risk Tolerability [22],
- ICAO Doc 10108 Aviation Security Global Risk Statement [23].

Best practice #4: Determining the cybersecurity baseline and gaps

When identifying risks, the organisation is advised to:

- define a security baseline, i.e. all cybersecurity standards applicable to the organization's activities. These standards may include:
  - IT hygiene rules and security best practices [24]: ANSSI recommendation guides, internal security rules, etc.,
  - standards: ISO/IEC 27002:2022 [25], etc.,
  - technical regulatory measures: Military Programming Law, Transposition of NIS Directives 1 and 2, II 901, IGI 1300, etc.
- identify any gaps versus this cybersecurity baseline in order to gain a clear picture of the organization's situation in terms of protection against information security risks and thus better determine the risks to which the organization is exposed.

In addition, the security baseline is updated during each iteration of risk assessment and treatment. Therefore, the organisation is advised to adopt a strategy of gradually increasing the level of requirements for this cybersecurity foundation:

- Step 1: Consider the ANSSI hygiene guide as the basic cybersecurity baseline and aim for compliance with the 42 measures:
  - IT Hygiene Guide, ANSSI, Version 2.0, September 2017 [24].
- Step 2: Consider a more demanding reference framework such as:
  - the measures of International Standard ISO/IEC 27002:2022 [25],
  - the measures of International Standard ISO/ISA/IEC 62443 [26],
  - the technical measures of the Military Programming Law [14], if applicable,
  - the technical measures of the transpositions of NIS Directives 1 [15] and/or 2 [42], if applicable.

Best practice #5: Information security incident management measures

In order to determine the technical and organizational measures to detect, respond and recover from an incident, the organisation is advised to refer to the following standards:

- Guides and best practices published by ANSSI,
- The measures set out in International Standard ISO/IEC 27002:2022 [25],
- ED-206-Guidance on Security Event Management, EUROCAE, 2022 [27].

Best practice #6: Identification of undesirable information security incidents

In order to identify undesirable information security incidents with a potential impact on aviation safety, the organisation is advised to rely on one or more reference frameworks, such as:

- Events that must be reported to the authority specified in Regulation (EU) 2015/1018,
- Security incident detection providers-Requirements reference framework, ANSSI, 2017-IV.2.2. b) [28],
- ETSI ISI Indicators standard (ISI 001-1 and Guides 001-2), ISI Event Model (ISI-002), ISI Maturity (ISI-003), ISI Event Detection (ISI-004)-5 standards on security incident detection, ETSI [29],
- International standard ISO/IEC 27035:2023-Information Technology-Information security incident management-Annex B [30],
- ED Decision 2023/009/R-Appendix I-Examples of threat scenarios with a potential harmful impact on safety [31],
- Mitre Attack-Reference to the tactics and techniques used in attack scenarios.

Best practice #7: Strategy for collecting information security events

When implementing a strategy for collecting information security events, the organisation is advised to refer to the following standards:

- Security incident detection providers-Requirements standard, ANSSI, 2017-IV.2.2. c) [28],
- Security recommendations for implementing a logging system, version 2, 2022, ANSSI [32],
- ED-206-Guidance on Security Event Management, EUROCAE, 2022 [27].

Best practice #8: Defining information security events detection rules

When defining detection rules, the organisation is advised to:

- rely on knowledge bases:
    - internal:
        - Audit results,
        - Penetration tests, vulnerability scans, and risks related to feared events.
    - external:
        - Threat and vulnerability monitoring,
        - Information security incidents known to other organizations,
        - Knowledge bases acquired from external partners.
- Formalize these rules, specifying for each of them:
    - means used to detect the event(s),
    - a description of the rule,
    - undesirable incident(s) that the rule aims to detect,
    - severity level of the event(s) to be detected.

Best practice #9: Defining immediate actions to respond to an information security incident

When defining the immediate actions to be taken in response to a security incident, the organisation is advised to identify:

- the resources to be activated within and outside the company, particularly in the context of:
  - a Security Operation Centre,
  - a contract with an ANSSI certified Security Incident Response Provider (PRIS)[5],
  - or membership of a CERT:
    - CERT Aviation France[6],
    - CERT-FR[7],
    - CSIRT[8].
- The technical and organizational measures that can be implemented to limit the spread of an attack and prevent the feared incident(s) from materializing. The organization can rely on:
  - ANSSI guide on cyberattacks and remediation: Managing remediation [33]-pages 33–35,
  - ED-206-Guidance on Security Event Management, EUROCAE, 2022 [27],
  - Guidance on Aviation Cybersecurity Incident Response & Recovery-ICAO (To be published).

Best practice #10: Defining recovery actions following a security incident

When developing the recovery procedure, the organisation is advised to refer to:

- ANSSI guide on cyberattacks and remediation: Managing remediation [33],
- ED-206-Guidance on Security Event Management, EUROCAE, 2022 [27],
- Guidance on Aviation Cybersecurity Incident Response & Recovery-ICAO (forthcoming).

Best practice #11: Secure transmission of sensitive information for notification to the competent authority

When the organization considers that sensitive information must be sent to the competent authority, the organisation is advised to:

- encrypt the information using a secure solution:
  - Zed! Container with a unique and robust password.
- send the secret and the key to access the secret via two different means of communication:
  - Secret: Zed! Container by email,
  - Key: Password via:
    - an encrypted messaging application, or,
    - in degraded mode by SMS, telephone, or hand delivery.

The organization contacts the entity in charge of its certificate/approval (DSAC-IR, DSAC-EC, and/or OSAC) to define the secure transmission methods.

Best practice #12: Technical references for third-party management

When managing third parties, it is recommended to rely on technical requirements standards such as:

- AirCyber Maturity Tool, Boostaerospace, 2023 [34],
- ISO 27001 standard [16].

Best practice #13: Subcontracting of ISMS activities

If an organisation subcontracts certain ISMS activities, the organisation is advised to use a service provider certified by ANSSI[5]. The latter is then considered to be in compliance with the requirements of Part-IS (IS.I/D.OR.250) provided that the following are also provided for:

- the possibility for the competent authority to have access to the subcontractor,
- the reporting to the organization of information security and vulnerability events having a potential impact on aviation safety in accordance with §4.4.1.2.2.

[5] In France, ANSSI certifies service companies, which offer guarantees of quality of service in terms of information security to the customers who use them. The list of these service providers and the standards with which they must comply are available on the ANSSI website: https://cyber.gouv.fr/produits-services-qualifies.

[6] CERT Aviation France: https://www.cert-aviation.fr/

[7] CERT–FR: https://www.cert.ssi.gouv.fr/

[8] Regional CSIRT: https://cyber.gouv.fr/csirt-territoriaux

Best practice #14: Background checks for verifying personnel trustworthiness

When the policy concludes that it is necessary for the organisation to verify the background of certain individuals, the organisation is advised to rely on existing mechanisms such as:

- prefectural authorization granted in connection with the issuance of an airport access pass,
- the provision of a criminal record extract,
- the National Defense secrecy protection system, when the status of the organisation allows it,
- any other existing system that meets the objectives of reliability control.

Best practice #15: Designing cybersecurity awareness training

When developing awareness sessions for staff, the organisation is advised to refer to the DSAC's guide to designing cybersecurity awareness sessions [35].

Best practice #16: Designing cybersecurity training

When developing training programs, the organisation is advised to refer to the DSAC's cybersecurity training guide [36].

Best practice #17: ISMS maturity models

When assessing the maturity of its ISMS, the organisation is advised to use one of the following maturity models:

- Cybersecurity Capability Maturity Model (C2M2), version 2.0,
- Cybersecurity Capability Maturity Integration,
- Systems Security Engineering-Capability Maturity Model (SSE-CMM),
- NIST Cybersecurity Framework (NIST CSF), version 1.1,
- ATM Cybersecurity Maturity Model, edition 1,
- Standard ISO/IEC 27004:2016-IS management – monitoring, measurement, analyses, and evaluation.

Best practice #18: Examples of elements or references in the security program

Procedures	3CFv3 Chapters
Risk management procedure (assessment, treatment, and monitoring)	4.1, 4.2, 4.3 and 6.1
Interface organisation management procedure	4.5.1
Background check procedure	5.1.1
Awareness monitoring procedure	5.3
Training monitoring procedure	5.4

Best practice #19: Examples of elements or references in the ISMS or SMS manual of the organisation

Procedures	3CFv3 Chapters
Risk management procedure (assessment, treatment, and monitoring)	4.1, 4.2, 4.3 et 6.1
Information security incident management procedure	4.4
Information security notification procedure	4.4.5
Interface organisation management procedure	4.5.1
Subcontractor management procedure for ISMS activities	4.5.2
Personnel reliability control policy	5.1.2
Awareness monitoring procedure	5.3
Training monitoring procedure	5.4
ISMS compliance evaluation procedure	6.2.1
ISMS effectiveness and maturity evaluation procedure	6.2.3
Continuous improvement procedure	6.3
Record keeping management procedure	7.1

Appendix II: Security essential functions for risk assessment

Function	Sub-function	Objective
Access control to critical areas	Access control for persons	Ensure only authorized individuals access security-restricted and critical zones
	Access control for vehicles	Prevent unauthorized vehicle entry into security-restricted and critical zones
Passenger and cabin baggage screening		Prevent introduction of prohibited items into aircraft cabin via passengers or their baggage
Hold baggage screening, protection, and reconciliation	Hold baggage screening	Detect and block prohibited items in checked baggage
	Protection of secured hold baggage	Prevent unauthorized access or tampering after security screening
	Baggage reconciliation	Ensure each piece of hold baggage corresponds to a boarded passenger
Staff and item screening		Ensure no prohibited items are introduced into secure zones by staff or their belongings
Cargo and mail screening		Prevent unauthorized access to air cargo and mail
Protection of secured cargo and supply warehouses		Ensure integrity and security of cargo and supplies in secured storage areas.
Information protection	Personnel vetting and access rights data	Protect sensitive information on background checks and access authorizations
	Processing and recording of data related to supply chain actors	Preserve integrity and confidentiality of data on supply chain participants
	Processing and storage of confidential security documents (e.g. security programmes and instructions)	Ensure confidentiality, integrity, and controlled access to sensitive aviation security documentation
Detection and interception of drones		Detect and neutralize unauthorized unmanned aerial systems in the vicinity of aviation operations

Appendix III: Safety essential functions for risk assessment

Production Organisation Approval (POA)

Function	Sub-function	Objective
Manage product configuration and compliance	Manage configuration of aircraft, components, and critical* systems	Ensure configurations remain compliant with the approved design definition
	Ensure compliance of products and parts with approved design and issue the certificate of conformity or authorized release certificate	Verify and certify that products and parts meet the approved design definitions
Ensure production quality	Industrialize and manage the production of critical* aircraft or components	Implement and control manufacturing processes to ensure compliance of products and parts
	Ensure robustness and traceability of critical* operations	Ensure all critical* operations are traceable and comply with safety requirements
	Manage the supply of critical* parts and materials and ensure the proper execution of subcontracted processes	Ensure that the supplied parts and components or the subcontracted processes comply with the approved design definition
	Verify traceability of critical* parts and materials	Verify that critical* parts and materials comply with the approved design definition.
Test, validate, and remediate non-conformities	Test and validate the product and its components	Conduct tests to ensure that products and components comply with safety requirements and/or the approved design definition
	Manage non-conformities and implement corrective actions	Identify and correct anomalies detected in production processes

**Are considered as "critical" the assets (components, systems or operations) assessed as critical during the risk assessment led on behalf of the safety management system*

Design Organisation Approval (DOA)

Function	Sub-function	Objective
Design, Develop, and Manage System Architectures	Define architecture and global configuration of the aircraft or system	Design architecture and configurations to ensure integration and compliance with requirements
	Manage configuration, changes, and technical data	Monitor configurations and disseminate data to ensure regulatory compliance
	Develop, integrate, and validate embedded software and systems	Design, integrate, and test embedded systems to ensure reliable operation
	Test and validate aircraft or system functions	Verify that all functions meet airworthiness and safety requirements
Manage design and test tools		Ensure tools and systems for design and testing are available, functional, and meet specifications
Manage certification processes		Organize and verify certification processes to ensure regulatory compliance

Airports

Function	Sub-function	Objective
Airport operations and traffic management	Maintenance of manoeuvring and traffic areas	Maintain the manoeuvring area and traffic areas to ensure the safe arrival and departure of aircraft
	Management of ground movement authorizations	Manage ground movement authorizations (traffic area, manoeuvring area, pedestrians, vehicles)
	Management of aircraft parking stand allocation	Manage aircraft parking stand allocation
Protection and maintenance of airport infrastructure	Securing airport surfaces	Secure obstacle limitation surfaces and the surroundings of the aerodrome
	Provision of airfield lighting	Ensure the operation of airfield lighting and report its operational status to the tower
Fire management		Ensure firefighter response in case of incidents
Aeronautical data management		Manage aeronautical data and information

Maintenance organisation (Part–145)

Function	Sub-function	Objective
Manage maintenance documentation, processes, and equipment	Manage approved documentation and airworthiness directives	Organize and monitor approved documentation and directives to ensure compliance and implementation.
	Manage tools and equipment used for maintenance	Ensure the availability, maintenance, and compliance of maintenance tools
	Ensure traceability of maintenance interventions	Record all interventions to ensure a complete and reliable history
	Manage the supply, inspection, and storage of aircraft parts and systems	Verify parts and systems compliance before their use on aircraft
Perform and inspect maintenance activities	Perform maintenance on aircraft and their components	Perform the necessary maintenance tasks to ensure the safety and airworthiness of aircraft
	Inspect and certify maintenance work	Verify compliance of work and issue release-to-service certificates
	Manage non-conformities and implement corrective actions	Identify and resolve detected anomalies to prevent safety risk

Continued Airworthiness Management Organisation (CAMO)

Function	Sub-function	Objective
Ensure continuous airworthiness of aircraft	Monitor aircraft airworthiness	Ensure ongoing compliance of aircraft with regulatory airworthiness requirements
	Monitor and implement airworthiness directives	Monitor and apply regulatory directives to ensure the safety of aircraft
	Manage approved modifications and repairs	Ensure modifications and repairs meet airworthiness standards
	Maintain technical and regulatory documentation	Ensure documentation is complete, up-to-date, and compliant
Plan and Supervise maintenance activities	Develop and manage aircraft maintenance programs	Define, approve, and update maintenance programs based on manufacturer's instructions, regulatory requirements, and operational needs
	Coordinate maintenance activities	Plan and coordinate maintenance interventions with MOAs and other entities
	Monitor traceability of maintenance operations	Ensure maintenance operations are fully and reliably documented.

Air operators (CAT/SPO/NCC)

Function	Sub-function	Objective
Management of aircraft and crews	Competency assessment and traceability of crew training	Assess competencies and trace the training of flight and cabin crew.
	Scheduling of aircraft and crews	Schedule aircraft and crews
	Assignment of aircraft and crews	Assign aircraft and crews to specific flights and ensure operational adjustments as needed.
Flight preparation	Flight planning	Develop the operational flight plan
	Filing the ATC flight plan	File the ATC flight plan
	Weight and balance & aircraft performances calculations	Prepare the weight and balance sheet and calculate aircraft performance
	Delivery of flight package to pilots	Deliver the flight package to pilots
Management of cockpit data and documentation	Access to necessary flight information	Allow pilots to access essential in-flight information (weather, NOTAMs, etc.)
	Display of navigation and aerodrome charts	Ensure navigation charts and tools are available, up-to-date, and reliable
	Access to emergency procedures documentation	Provide pilots with integrated emergency procedures documentation

Approved Training Organisation (ATO) & Flight Simulation Training Device Operators (FSTD)

Function	Sub-function	Objective
Manage training data	Manage in-flight training programs	Provide pilot trainees with a comprehensive and uncompromised flight training program
	Manage pilot theoretical training material	Provide pilot trainees with an uncompromised theoretical training material that meets regulatory requirements.
	Track training paths	Ensure the traceability and progression of the training followed by each pilot trainee.
Manage aircraft used for training		Provide aircraft that meet safety standards for flight training
Manage flight simulators used for pilot training		Provide Flight Simulation Training Devices (FSTDs) that meet safety requirements for the training of pilot trainees.

Aeromedical centre (Pilots and ATCO)

Function	Sub-function	Objective
Ensure the implementation and quality of mandatory medical examinations for pilots and air traffic controllers	Conduct mandatory medical examinations for pilots and air traffic controllers.	Verify that pilots and air traffic controllers meet the necessary medical criteria to perform their duties and issue a medical certificate.
	Ensure the availability of medical equipment that complies with aeromedical standards and is properly calibrated for examinations.	Ensure the accuracy and reliability of medical examinations through equipment that meets regulatory requirements
	Ensure traceability and protect the data of medical examinations and medical certificates	Ensure rigorous monitoring of examinations, and the integrity and confidentiality of medical data.

Approved Training Organisation (ATCO)

Function	Sub-function	Objective
Manage training data	Manage ATCO training programs	Provide ATCO trainees with a comprehensive and uncompromised training program
	Manage theoretical training material	Provide ATCO trainees with an uncompromised theoretical training material that meets regulatory requirements.
	Track training paths	Ensure the traceability and progression of the training followed by each trainee.
Manage ATC simulators used for training		Ensure the availability of ATC simulators that comply with safety standards for the practical training of ATCO trainees

Air Navigation Service Provider (ANSP)

Function	Sub-function	Objective
Air Traffic Management (ATM)	Air Traffic Services (ATS)	Ensure flight safety, regularity, and efficiency. Includes ATC, alerting service, and flight information
	Air Traffic Flow Management (ATFM)	Balance demand and capacity of traffic management services to prevent congestion and minimize delays
	Airspace Management (ASM)	Strategically and tactically manage airspace to ensure its efficient and safe use
Communication, Navigation, Surveillance (CNS)	Communication (COM)	Ensure effective information exchange between air traffic controllers and pilots to maintain safe and orderly air traffic
	Navigation (NAV)	Enable aircraft to determine their position accurately and follow predefined flight paths.
	Surveillance (SUR)	Enable real-time monitoring of aircraft positions to ensure safe separation between them
Provision of meteorological information (MET)		Provide real-time weather conditions and alerts to aircraft and air traffic controllers
Aeronautical Information Service (AIS)		Collect, manage, and disseminate information necessary for the safety, regularity, and efficiency of air navigation

U-Space Service Provider (USSP)

Function	Sub-function	Objective
Develop and implement the means to provide U-space services to drone operators		Design, deploy, and maintain the technical means essential for the provision of U-space services
Provide U-space services to drone operators		Ensure the availability and efficiency of U-space services to enable safe and regulation-compliant drone operations.

Flight Procedures Design (FPD)

Function	Sub-function	Objective
Design and validate flight procedures	Design procedures in compliance with regulations	Ensure that flight procedures comply with regulations and take operational constraints into account.
	Validate and verify procedures before implementation	Ensure that the procedures are comply with safety requirements, and are adapted to operational constraints

Appendix IV: Compliance matrix

Cyber Compliance Framework v3			Reg. (UE) 2015/1998 [1] Reg. (CE) 300/2008 [37] AIM [38] Code of transports [39]	Part-IS.I/D.OR	AMC IS.I.OR [40]
3. Governance	3.1. Commitment of the Accountable Manager			200 a) 1)	200 a) 1)
	3.2. Information security policy			200 a) 1) et d) 240 a) 2)	200 a) 1) 240 a) 2)
	3.3. Resource Management, Roles, and Responsibilities			240 a) 1) et 3) 240 b) à (f) 240 (h)	240 a) 3) et b) 240 d), f) et h)
4. Information Security Risk Management			1998 – 1.7.1, 1.7.2 et 1.7.3	205 c)	
	4.1. Establishing the context		1998 – 1.7.1, 1.7.2 et 1.7.3	205 a) 1)	
	4.2. Risk assessment		1998 – 1.7.1, 1.7.2 et 1.7.3 AIM – DR-1-7-1 (I)	205 a), b), c) et e) 210 b)	205 a), b), c) et e)
	4.3. Risk treatment		1998 – 1.7.1, 1.7.2 et 1.7.3	210 a) et b)	210 a)
	4.4. Information security incident management		1998 –1.7.2	200 a) 5)	
		4.4.1. Detection of information security incidents		215 a), b), et e) 220 a) 230 b) et c) 1)	215 a) et b) 220 a)
		4.4.2. Information security incident response		220 b)	220 b)
		4.4.3. Recovery		220 c)	220 c)
		4.4.4. Notification to the competent authority		230 a), b) et c)	230 a) et b) 230 c)
	4.5. Third-party risk management	4.5.1. Interfacing organisations	AIM – B-2 AIM – B-4	200 a) 13) 215 c) et d) 230 a), b) et c)	200 a) 13)
		4.5.2. Subcontracting of ISMS activities		235 a) et b)	235 a) et b)
5. Personnel and competencies	5.1. Background checks and trustworthiness control		1998 – 11.1.2 c), 11.1.3, 1998 – 11.1.7 CT – L6342-3,R6342-32&33	240 i)	240 i)
	5.2. Awareness		1998 – 11.2.1.4, 11.2.8.1 et 11.2.8.2 AIM 11-2-1-4 et 11-2-1-5	240 h)	
	5.3. Training		1998 – 11.2.1.4, 11.2.8.1 et 11.2.8.2 AIM 11-2-1-4 et 11-2-1-5	240 g)	240 g)
6. Definition and operation of the ISMS	6.1. Information security risk management monitoring		1998 – 1.7.1, 1.7.2 et 1.7.3 AIM DR 1-7-1 (II) et B-3	200 a) 2) à 6) 200 a) 8) à 10) 205 d)	205 d)
	6.2. Evaluation of the ISMS	6.2.1. Evaluation of ISMS compliance		200 a) 12)	200 a) 12)
		6.2.2. Response to findings notified by the competent authority		200 a) 7) 225 a) et b)	225
		6.2.3. Evaluation of ISMS effectiveness and maturity		260 a)	260 260 a)
	6.3. Continuous improvement of the ISMS			200 b) 260 b)	260 260 b)
	6.4. Changes to the information security management system			200 c) 250 c) 255 a) et b)	200 c) 255
7. Record keeping	7.1. Procedure of record keeping			200 a) 11) 245 c) et d)	245 c) et d)
	7.2. Records to keep			200 a) 11) 245 a) et b)	245 a) 1) vi) et a) 5)
8. Documentation	8.1. Security Program		1998 – 1.7.1, 1.7.2 et 1.7.3 300 – 12,13 et 14		
	8.2. Information security management system Manual			250 a) et d)	
DSAC Communications [12] **BI OSAC 2025–03** [13]				200 e) 250 b)	200 e)

Appendix V: Definitions

Authenticity is the property that an entity is what it claims to be.		ISO/IEC 27000:2018 [41]
The **Accountable Manager** is the person authorized to ensure that all activities of their organisation are funded and carried out in compliance with applicable requirements. This person is responsible for establishing and maintaining an effective management system.		Regulation (EU) 2017/373 [10]
Availability is the property of being accessible and usable upon demand by an authorized entity.		ISO/IEC 27000:2018 [41]
Aviation safety is the state in which risks associated with aviation activities involving or supporting aircraft operations are reduced and controlled to an acceptable level.		Annex 19: ICAO [45]
Aviation security combines measures and human and material resources to protect civil aviation against unlawful interference, aiming to prevent acts of malicious intent targeting aircraft, passengers, and crew members.		Annex 17: ICAO [46]
A **Competent Authority**: one or more entities designated by a Member State and having the necessary powers and allocated responsibilities for performing the tasks related to certification, oversight and enforcement in accordance with this Regulation and with the delegated and implementing acts adopted on the basis thereof, and with Regulation (EC) n° 549/2004		Regulation (EU) 2018/1139 [42]
Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.		ISO/IEC 27000:2018 [41]
A **Contractor** is an external entity with its own approval and performing tasks under this approval on behalf of an individual or another approved organisation. In production contexts, this entity is typically referred to as a supplier.		Guide P-03-01 Ed0: DSAC/OSAC [43]
An **essential function** refers to:	essential assets,	EBIOS RM [17]
	business values: In the context of the study, business values are important components for the organisation in accomplishing its mission. This can include a service, a support function, a project stage, and any associated information or know-how	EBIOS RM [17]
	critical assets: representing value to the organisation, such as information, processes, and business activities.	ISO/IEC 27002:2022 [25]
An **incident** means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems;		Directive (EU) 2022/2555 [44]
Information security involves preserving the confidentiality, integrity, authenticity, and availability of networks and information systems.		Delegated Regulation (EU) 2022/1645 [3]
An **information security event** means an identified occurrence of a system, service or network state indicating a possible breach of the information security policy or failure of information security controls, or a previously unknown situation that can be relevant for information security;		Delegated Regulation (EU) 2022/1645 [3]
An **information security risk** is the risk posed to civil aviation activities, assets, individuals, and other organisations by a potential information security event. These risks are associated with the possibility of threats exploiting vulnerabilities in an information asset or group of assets.		Delegated Regulation (EU) 2022/1645 [3]
Integrity is the property of accuracy and completeness.		ISO/IEC 27000:2018 [41]
An **interface** is a common boundary between two systems, allowing exchanges between them.		LAROUSSE
Network and information system' means: (a) an electronic communications network as defined in Article 2, point (1), of Directive (EU) 2018/1972, (b) (b) any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data; or (c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance.		Directive (EU) 2022/2555 [44]

A **subcontractor** is an external entity performing specified tasks for an approved organisation under its approval. Subcontracting involves delegating part of an activity or contract to another company, which executes a product or task based on instructions from the ordering organisation while maintaining control over the product and its characteristics. This distinguishes subcontractors from suppliers, who have full responsibility for the products or services they offer to their clients.	Guide P-03-01 Ed0: DSAC/OSAC [43]
A **supplier** is an external entity providing products or services for which it has full responsibility.	Guide P-03-01 Ed0: DSAC/OSAC [43]
A **threat** is a potential violation of information security, existing when an entity, circumstance, action, or event could cause harm.	Delegated Regulation (EU) 2022/1645 [3]
A **vulnerability** is a flaw or weakness in an asset or system, procedures, design, implementation, or information security measures that could be exploited, resulting in a breach of the information security policy.	Delegated Regulation (EU) 2022/1645 [3]

Appendix VI: Acronyms

3CF	Cadre de conformité cyber France – Cyber Compliance Framework
AIM	Arrêté InterMinistériel – Interministerial order
AM	Accountable Manager
ANSP	Air Navigation Service Provider
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information – French information security agency
ATCO – TO	Air Traffic COntroller - Training Organisation
ATM/ANS	Air Traffic Management / Air Navigation System
BI OSAC	Bulletin Information OSAC – Information letter OSAC
CAMO	Continuing Airworthiness Management Organisation
CAT	Certificate of Air Transport
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
DOA	Design Organisation Approval
DSAC	Direction de la Sécurité de l'Aviation Civile – French Civil Aviation Authority
EASA	European Aviation Safety Agency
EC	European Commission
ECCAIRS	European Co-ordination Centre for Accident and Incident Reporting Systems
EU	European Union
EUROCAE	European Organisation for Civil Aviation Equipment
FDP	Flight Procedure Design Organisation
FSTD	Flight Simulation Training Device
ICAO	International Civil Aviation Organisation
IGI	Instruction Générale Interministérielle – General Interministerial instruction
II	Instruction Interministérielle - Interministerial instruction
ISMS	Information Security Management System
METEOR	Module d'Échange et de TÉlétransmission avec les ORganismes
NCC	Non-Commercial Complex
NIS	Network and Information Security
POA	Production Organisation Approval
SMS	Safety Management System
SPO	Specialised Operations

Appendix VII: References

[1]	Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on civil aviation security
[2]	Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 laying down detailed rules for the implementation of Regulation (EU) 2018/1139 of the European Parliament and of the Council as regards the requirements for information security risk management with a potential impact on aviation safety
[3]	Delegated Regulation (EU) 2022/1645 of 14 July 2022 laying down detailed rules for the implementation of Regulation (EU) 2018/1139 of the European Parliament and of the Council as regards the requirements for information security risk management with a potential impact on aviation safety
[4]	Commission Regulation (EU) No 748/2012 of 3 August 2012 laying down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts, and appliances, as well as for the certification of design and production organisations
[5]	Commission Regulation (EU) No 139/2014 of 12 February 2014 laying down requirements and administrative procedures related to aerodromes
[6]	Commission Regulation (EU) No 1321/2014 of 26 November 2014 on the continuing airworthiness of aircraft and aeronautical products, parts, and appliances, and on the approval of organisations and personnel involved in these tasks
[7]	Commission Regulation (EU) No 965/2012 of 5 October 2012 laying down technical requirements and administrative procedures related to air operations
[8]	Commission Regulation (EU) No 1178/2011 of 3 November 2011 laying down technical requirements and administrative procedures related to civil aviation aircrew
[9]	Commission Regulation (EU) 2015/340 of 20 February 2015 laying down technical requirements and administrative procedures related to air traffic controller licenses and certificates
[10]	Commission Implementing Regulation (EU) 2017/373 of 1 March 2017 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight
[11]	Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space
[12]	DSAC communication-METEOR: - Airports: n°37820 - Air navigation service providers: n°37940 - Air operators and ATO: n°37760 - Aeromedical centre: Letter 25-011/DSAC/PN et 25-075/DSAC/ANA
[13]	BI OSAC 2025-03: Implementation of regulations (EU) 2022/1645 et (UE) 2023/203 relating to Part-IS
[14]	Order of 11 August 2016 laying down the security rules and declaration procedures for vital information systems and security incidents related to the vital activity sub-sector "Air Transport" and implementing Articles R. 1332-41-1, R. 1332-41-2, and R. 1332-41-10 of the Defense Code, Legifrance, August 2016)
[15]	Decree No. 2018-384 of 23 May 2018 on the security of networks and information systems of essential service operators and digital service providers, Legifrance, May 2018
	Order of 13 June 2018 setting the terms of the declarations provided for in Articles 8, 11 and 20 of Decree no. 2018-384 of 23 May 2018 on the security of the networks and information systems of essential service operators and digital service providers, Legifrance, June 2018
	Order of 1 August 2018 on the cost of an inspection carried out by the Agence nationale de la sécurité des systèmes d'information pursuant to Articles 8 and 14 of Law no. 2018-133 of 26 February 2018 containing various provisions for adapting to European Union law in the field of security, Legifrance, August 2018
	Order of 14 September 2018 setting the security rules and deadlines mentioned in Article 10 of Decree no. 2018-384 of 23 May 2018 on the security of the networks and information systems of essential service operators and digital service providers, Legifrance, September 2018
[16]	International Standard ISO/IEC 27001:2022-Information security, cybersecurity, and privacy protection-Information security management systems
[17]	EBIOS Risk Manager Guides ANSSI Version 1.5 March 2024
[18]	International Standard ISO/IEC 27005:2022-Information security, cybersecurity, and privacy protection-Guidelines for information security risk management
[19]	IACO/GCRC risk assessment methodology-June 2025 (RESTRICTED)
[20]	International Standard ISO/IEC 31000:2018-Risk Management-Guidelines
[21]	White paper: Identification and Classification guidance for Part-IS assets-ED/DO-ISMS Guidance for Aviation EUROCAE WG-72 / RTCA SC-216 2023
[22]	ICAO Doc 9859 Safety Risk Tolerability
[23]	ICAO Doc 10108 Aviation Security Global Risk Statement
[24]	ANSSI Guide to IT Hygiene Version 2.0 September 2017
[25]	International Standard ISO/IEC 27002:2022-Information security, cybersecurity, and privacy protection-Information security controls
[26]	International Standard ISA/IEC 62443-Series of Standards

[27]	ED-206-Guidance on Security Event Management EUROCAE 2022
[28]	Security Incident Detection Service Providers-Requirements Framework ANSSI 2017
[29]	Standard ETSI ISI Indicators (ISI 001-1 and Guides 001-2) ISI Event Model (ISI-002) ISI Maturity (ISI-003) ISI Event Detection (ISI-004)-5 standards on security incident detection ETSI
[30]	International Standard ISO/IEC 27035:2023-Information Technology-Information security incident management
[31]	ED Decision 2023/009/R EASA 2023
[32]	Security recommendations for the implementation of a logging system-version 2, ANSSI, 2022
[33]	ANSSI guide on cyberattacks and remediation: Managing remediation, ANSSI, 2025
[34]	AirCyber Maturity Tool Boostaerospace 2023
[35]	Guide de conception de sessions de sensibilisation cybersécurité_v1_DSAC_2021
[36]	Guide de formation cybersécurité_v1_DSAC_2021
[37]	Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security
[38]	Order of September 11,2013 relating to civil aviation security measures
[39]	Code of transports
[40]	Easy Access Rules for Information Security EASA June 2024
[41]	International standard ISO/IEC ISO/IEC 27000:2018
[42]	Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation
[43]	P-03-01-Instruction and monitoring of organisation approvals with management system DSAC/OSAC 2024
[44]	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union
[45]	Annex 19: ICAO
[46]	Annex 17: ICAO

Direction générale de l'Aviation civile
Direction de la Sécurité de l'Aviation civile
50, rue Henry Farman
75720 PARIS CEDEX 15
Tél.: +33 (0)1 58 09 43 21
www.ecologie.gouv.fr