Guidance material to Part-IS oversight

1. References

- Commission Regulation (EU) No 139/2014 of 12 February 2014 laying down requirements and administrative procedures related to aerodromes pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council and its amendments
- Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 748/2012 and (EU) No 139/2014 and amending Commission Regulations (EU) No 748/2012 and (EU) No 139/2014
- Executive Director Decision 2023/009/R of 12 July 2023 issuing Issue 1 of the Acceptable Means of Compliance and Guidance Material to the Annex (Part-IS.D.OR) to Commission Delegated Regulation (EU) 2022/1645 'AMC and GM to Part-IS.D.OR — Issue 1' 'Management of information security risks — AMC & GM to Part-IS.D.OR and Part-IS.I.OR'
- 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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148
- Commission Implementing Regulation (EU) 2019/1583 of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures
- Law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security, transposing Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 in Belgium
- ADR.OR.B.040 Changes
- ADR.OR.D.005A Information security management system
- And their related AMC and GM
- Circular GDF-14: Guidelines regarding the form and administrative procedures for the certification and supervision of aerodromes

2. Abbreviations

- AMC Acceptable Means of Compliance
- AVSEC Aviation Security, and by extension, the regulation that applies to
- BCAA Belgian Civil Aviation Authority
- GM Guidance Material
- IS Information Security
- ISMS Information Security Management System
- ISMM Information Security Management System Manual

3. Introduction

The Commission Delegated Regulation (EU) No 2022/1645 lays down requirements for the management of information security risks with a potential impact on aviation safety for organisations for the aerodromes.

The BCAA has developed this guidance material for the national industry to ensure appropriate implementation of the information security management system and proper integration with the existing management system of the aerodromes.

This document is in no way replacing the requirements from the regulation.

4. Scope of Part-IS

4.1. Part-IS, a safety-related regulation

The Part-IS regulation sets out the requirements to be met by the organisations in order to identify and manage information security risks with potential impact on aviation safety which could affect information and communication technology systems and data used for civil aviation purposes and to detect information security events and identify those which are considered information security incidents with potential impact on aviation safety and respond to, and recover from, those information security incidents.

The definition of information security used for this purpose should not be interpreted as divergent from the definition of security of network (communication pathways) and information systems (software, hardware and processes that store, process and manage aviation data) as laid down in Directive (EU) 2022/2555.

It is important to emphasize the scope of the information security management system (ISMS), especially considering the existence of other regulations dealing with information security:

- AVSEC, related to aviation security;
- NIS2, related to business continuity or resilience; and
- Part-IS, related to aviation safety.

The Part-IS regulation is not to be considered an isolated IT concern or a standalone structure requiring separate development. Instead, it should be viewed as a component to the organizations existing management system. The regulation is intended to extend the scope of the organisations management system regardless of, if this is developed by the organisation itself or contacted to a third party.

To conclude, Part-IS is a safety regulation that considers one extra cause having safety consequences to be considered. It does not establish new safety requirements and is integral to traditional principles of risk management.

4.2. Part-IS, a scope to be defined

Part-IS requires organisations to identify and assess the risks to all relevant assets to ensure a comprehensive information security framework. This involves understanding how these assets are interconnected and how a vulnerability in one area could impact others.

Indeed, aviation is an interconnected, complex environment with multiple critical suppliers and service providers. It is important for an aerodrome to understand its critical supply chain for the provision of essential services and the methods of connections into its critical system environments.

5. Expectations from aerodromes and oversight by the BCAA

Before the applicability date of October 16th 2025, aerodrome operators should have:
- Implemented the ISMS at least at “Present” and “Suitable” levels;
- Performed a compliance assessment to ensure the organisation meets the requirements set out by the regulation.

5.1. BCAA oversight planning steps

5.1.1. Step 1

To enable the BCAA to assess whether the organisation has demonstrated implementation of an ISMS at the "Present" and "Suitable" levels, and is prepared to operate the ISMS effectively, aerodrome operators shall make the following documentation available:

1. The first version of their "Information Security Management Manual (ISMM)", which may be integrated in other manuals, policies or procedures according to Appendix 1 in chapter 8;
2. The procedure for managing changes in the ISMS, as described under Part-IS points IS.D.OR.255, that may be part of the ISMM or integrated into an existing change procedure according to chapter 7;
3. An initial risk assessment identifying:
    a) The aerodrome's activities, facilities and resources, as well as the services it operates, provides, receives or maintains;
    b) The equipment, systems, data and information that contribute to the functioning of the elements listed in point (a) above;
    c) The interfaces that it has with other organisations, and which could result in the mutual exposure to information security risks;

    This (a), (b), (c) information being part of the document called "Inventory of assets" established according to Appendix 2 in chapter 9;

    d) The major risks and related threat scenarios, both internal and at the interfaces with other organisations, being part of the document called "Risk assessment" according to Appendix 3 in chapter 10;

    These last 2 documents will help the BCAA to understand:

    - Which digital assets are used in the aerodrome aviation-related activities;
    - Whether those assets are critical to aviation safety;
    - What cybersecurity risks are associated with those safety-critical assets.

4. Evidence that internal compliance monitoring activities have taken place, via a document provided by the BCAA, called "Part-IS compliance self-assessment" according to Appendix 4 in chapter 11.

The documentation shall be provided to the BCAA via a change requiring prior approval, as prescribed by *ADR.OR.B.040 Changes* and *ADR.OR.D.005A Information security management system* to allow formal approval of the initial version of the ISMM and the procedure for managing changes in the ISMS.

Depending on when the aerodrome makes the documentation available to the BCAA, several cases may occur:

- **Case 1**: The aerodrome has made available the documentation to the BCAA sufficiently in advance, allowing the BCAA to approve the ISMM and the procedure described under Part-IS point IS.D.OR.255 and to assess the rest of the documentation by the applicability date.
- **Case 2**: The aerodrome has made available the documentation to the BCAA before the applicability date but has not provided sufficient time to allow the approval the ISMM and the procedure described under Part-IS point IS.D.OR.255 and to assess the rest of the documentation by the applicability date. In this case, and while the BCAA if still performing the assessment, the aerodrome may continue operation and implementation, unless any findings already identified by the authority justify the need for limitations.
- **Case 3:** The aerodrome has not made available the documentation to the BCAA by the applicability date. In this case, the BCAA will raise a level 2 finding indicating that the aerodrome has not provided any proof of compliance with ISMS requirements. Depending on the reactivity of the aerodrome in sending the documents described above, and a preliminary review of the documents (if/when received), the BCAA may allow the aerodrome to continue operating normally or may impose limitations, for the duration of the finding.

5.1.2. Step 2

The “Operating” level will be assessed through an initial oversight planned after the applicability date.

5.1.3. Step 3

The “Effective” level[1], as well as the continuous compliance, will be assessed through continuous oversight.

6. Complexity and proportionality of the ISMS

Considering the complexity of the aerodromes in terms of:

- **Position in the functional chain** and number of interfacing organisations/stakeholders;
- **Complexity of the organisational structure and hierarchies**; and
- **Complexity of the information and communication technology systems and data** used and their connection to external parties;

the aerodromes in the scope of this regulation are **considered as complex** organisations and no derogation is possible in the framework of Part-IS. This complexity and the overlap between Part-IS, AVSEC and NIS2 determines the proportionality of the ISMS implementation.

In terms of risk assessment and treatment, the aerodromes are expected to:

- Perform detailed risk assessments; and
- Review it frequently.

In terms of governance structure, the aerodromes are expected to have:

- Governance committees in place, to ensure alignment with the organisation’s safety and security objectives, and should include representation from senior management, IT, legal, and key business units;
- Comprehensive metrics and reporting structures to track the effectiveness of the ISMS as well as reporting on key performance indicators and resource allocation;
- Detailed and harmonised policies and procedures to cover various business units, compliance requirements, and operational processes, including specialised policies for areas like cloud security, third-party management, and mobile device management.

In terms of training program, the aerodromes are expected to have:

- Extensive role-based training programs tailored to different functions within the organisation;
- Security awareness campaigns using various methods (e.g. phishing simulations, workshops, e-learning modules) continuously deployed to keep security top-of-mind for all employees across the organisation;

In terms of contracted activities, the aerodromes are expected to have:

- Security assessments of contracted organisations and ongoing monitoring of third-party risks;
- Security requirements integrated into contracts;
- Regular audit of contracted organisations in order to ensure they comply with the organisation’s security objectives.

[1] “Effective” level corresponds to the subsequent “continuous improvement” that should be pursued by the organisation once compliance with the requirements has been achieved. In this regard, and for the purpose of complying with the “Continuous Improvement” requirements contained in points IS.I.OR.260 and IS.D.OR.260 of Part-IS, the concept of “maturity” is introduced.

In terms of incident management, the aerodromes are expected to establish:

- A dedicated Security Operations Centre (SOC) to monitor security events, manage incidents, and coordinate response efforts across the organisation;
- A detailed incident response plans that cover a variety of scenarios, including cross-departmental coordination, communication strategies, and operational continuity planning;
- Crisis simulation exercises that involve key stakeholders across the organisation to test the effectiveness of incident response and operational continuity plans.

In terms of continuous improvement and compliance monitoring, the aerodromes are expected to:

- Conduct regularly comprehensive internal audits to assess compliance with the ISMS and identify areas for improvement;
- Implement a continuous improvement process to update and refine the ISMS based on audit findings, incident post-mortems, and changes in the threat landscape.

In terms of record keeping and documentation, the aerodromes are expected to:

- Maintain an extensive documentation of all ISMS processes, risk assessments, incident reports, and compliance activities;
- Collect, retain and securely store accessible records and data, over extended periods.

In terms of security technologies, the aerodromes are expected to:

- Use security technologies to help manage the monitoring, detecting, and responding to security incidents across the organisation;
- Implement threat intelligence to enable threat detection and response across the broad threat surface.

7. Management of changes

7.1. Management of change explained

In the scope of reg. EU 139/2014 ADR.OR.B.040, a change is defined as any planned action in the organisation, infrastructures or equipment, including the introduction of new procedures and modifications of existing procedures, or the entry into force of new regulations which:

- affect the safety of the aerodrome and
- its management is not established in advance in the day-to-day operation of the aerodrome operator, meaning by an existing procedure of the aerodrome manual.

This definition can be extended to the framework of Part-IS, where information security is seen as a cause that directly impacts aviation safety.

From AMC1 IS.D.OR.200(a)(1), a significant change is defined as a notable alteration or modification that has an meaningful impact on the organisation’s operations, such as a structural change within the organisation due to reorganisations, a change in the business processes (e.g. working from home, use of personal devices), a technological evolution (e.g. distributed computing resources, artificial intelligence/machine learning) or an evolution in the threat landscape.

By analogy to aviation safety, a change is defined regarding to its impact on the information security management system.

Examples of changes that have an impact on the ISMS:

- The organisation integrates another company within its organisational structure;
- The organisation has identified non-conformities indicating an incorrect scope;

- The organisation contracts information security management activities as per IS.OR.235;
- The organisation implements changes to their risk treatment methodology;
- The organisation changes its incident recovery procedure.

Examples of changes with no impact on the ISMS:

- The organisation replaces the software tool for encrypting sensitive files with another IT solution;
- The organisation decides to update an existing preventive control e.g. configuring a new firewall in its internal network;
- Update in the staff training content as a result of the continuous improvement processes established within the organisation.

7.2. Changes requiring prior approval by the BCAA

In line with the aviation safety regulation, any change:

- affecting the Part-IS compliance status of the aerodrome;
- affecting a safety-critical aerodrome equipment; or
- significantly affecting elements of the information security management system;

shall require prior approval by the Competent Authority.

Aerodrome operators shall implement this scope for changes requiring prior approval. This scope is suggested to include the items:

a) Use of alternative means of compliance (IS.D.OR.250)
b) Change to the procedure for management of changes (IS.D.OR.255)
c) Change to the aerodrome that has an impact on compliance status of the aerodrome with regard to Part-IS
d) Change to information security safety-related equipment
e) Change that significantly affects elements of the information security management system, including the designation of the accountable manager or the common responsible person if applicable
f) Change in the scope of the information security management system, including new safety-critical asset or new safety risk of an existing asset
g) Change in the contracted activities that fulfil part of the Part-IS requirements compliance

7.3. Changes requiring prior notification to the BCAA

The aerodrome's procedure for management of changes shall describe the scope of changes requiring prior notification to the BCAA and shall contain as a minimum:

- Change of appointed persons (compliance monitoring manager, IS manager or responsible person);
- Change in the cybersecurity controls that might affect the organisation compliance (including maturity)**;**
- Change in procedures or policies demonstrating compliance with Part-IS requirements (except the prior approval ones);
- Amendment of the ISMM.

7.4. Procedure for managing changes

According to IS.D.OR.255, to enable an organisation to implement changes without prior approval of the Competent Authority, the Competent Authority shall approve a procedure defining the scope of such changes and describing how such changes will be managed and notified.

Any change, even those not requiring prior approval by or prior notification to the BCAA, shall be reviewed and internally approved by the organisation prior to implementing it.

The procedure for managing the changes as foreseen in IS.D.OR.255 shall define:

- The way to request for change,
- The risk assessment to be done,
- The internal approvement process,
- The criteria for approval of notification to the BCAA,
- The documentation and record keeping of the changes.

The procedure for managing the changes shall follow the prescriptions of GDF-14.

8. Appendix 1 – ISMS manual (ISMM)

It is highly recommended that the ISMS manual, or ISMM, is integrated as much as possible to the existing aerodrome manual. In this case, a clear cross reference shall be made available to the BCAA, that indicates which documents correspond to the different requirements.

As prescribed by IS.D.OR.250, the ISMM or any other policies and procedures shall contain the following items:

1. A statement signed by the accountable manager confirming that the organisation will at all times work in accordance with the Part-IS and the ISMM requirements;
2. The title(s), name(s), duties, accountabilities, responsibilities and authorities of the person or persons referred to in point IS.D.OR.240(b) and (c);
3. The title, name, duties, accountabilities, responsibilities and authorities of the common responsible person referred to in point IS.D.OR.240(d), if applicable;
4. The information security policy of the organisation as referred to in point IS.D.OR.200(a)(1);
5. A general description of the number and categories of staff and of the system in place to plan the availability of staff as required by point IS.D.OR.240;
6. The title(s), name(s), duties, accountabilities, responsibilities and authorities of the key persons responsible for the implementation of point IS.D.OR.200, including the person or persons responsible for the compliance monitoring function referred to in point IS.D.OR.200(a)(12);
7. An organisation chart showing the associated chains of accountability and responsibility for the persons referred to in points (2) and (6);
8. The description of the internal reporting scheme referred to in point IS.D.OR.215;
9. The procedures that specify how the organisation ensures compliance with Part-IS, and in particular:
   (i) The documentation in point IS.D.OR.200(c), in particular:
      a. The procedure for identifying, reviewing and mitigating risks referred to in point IS.D.OR.200(a)(2) & (3);
      b. The procedure for detecting information security events, and identifying, responding to, and recovering from, the information security incidents referred to in point IS.D.OR.200(a)(5);
      c. The procedure for implementing an immediate reaction to an information security incident or vulnerability with an impact on aviation safety referred to in point IS.D.OR.200(a)(6);
      d. The procedure for managing findings raised by the BCAA referred to in point IS.D.OR.200(a)(7);
      e. The procedure for external reporting referred to in point IS.D.OR.200(a)(8);
      f. The procedure for complying with requirements laid down in point IS.D.OR.240, especially in terms of competence of the personnel, acknowledgement of their responsibilities and insurance of their identity and trustworthiness referred to in point IS.D.OR.200(a)(10);
      g. The procedure for record-keeping referred to in point IS.D.OR.200(a)(11);
      h. The procedure for monitoring compliance of the organisation referred to in point IS.D.OR.200(a)(12);
      i. The procedure for protecting the confidentiality of information referred to in point IS.D.OR.200(a)(13);

   (ii) The procedure for continuous improvement referred to in point IS.D.OR.200(b)

   (iii) The procedures that define how the organisation controls any contracted activities referred to in point IS.D.OR.200(a)(9);

(iv) The procedure for the amendment of the ISMM;

10. The details of currently approved alternative means of compliance.

Please consider the possible use of existing resources (policies) made available by the CCB that can be adapted to Part-IS and available in 3 languages.

9. Appendix 2 – Inventory of assets

9.1. Preamble

Effective asset management protects the organisation's information security by detecting vulnerabilities and managing threats and helps to protect assets' integrity, availability, and confidentiality.

Asset identification enables the organisation to develop a thorough inventory of all hardware, software, data repositories, and network resource, including third-party connections. Once identified, the assets are categorised based on their criticality and sensitivity. This helps prioritise the security measures and allocate appropriate resources based on the value and importance of each asset, and especially their safety significance.

9.2. What is an asset?

An asset is defined as anything that has value to an organisation and is therefore susceptible to information security risks. This includes not just physical objects, but also intangible items such as data. Essentially, any part of network and information systems that could be compromised and negatively impact the organisation's ability to operate safely resorts under the definition of an asset.

Assets can be detailed as:

- Hardware such as, laptops, servers, printers, cell phones, USB sticks, authentication keys, and network infrastructure;
- Software;
- Information such as data including sensitive information, procedures and workflows related to safety-critical operations.

Asset definition can be broaden to other organisation's assets such as intellectual property, brand reputation, personnel, infrastructure and outsourced services. Nevertheless, the Part-IS regulation requests the organisation to identify the assets and the associated vulnerabilities that could affect aviation safety.

9.3. Inventory of assets

In the framework of Part-IS, the assets should be identified from:

- The aerodrome's activities, facilities and resources, as well as the services it operates, provides, receives or maintains (further referred as "function");
- The equipment, systems, data and information that contribute to the functioning of the elements listed above (further referred as "building blocks" of a function);
- The interfaces that it has with other organisations, and which could result in the mutual exposure to information security risks.

The inventory of assets should be thought and kept as a tool to manage safety risks, at a functional level. It means that to each function, the inventory of assets should list the constituting building blocks in terms of hardware, software and data (or information)[2]. It does not intend to list all and every IT devices used by the aerodrome.

[2] The philosophy developed by the BCAA is inspired from the UK CAA document "Cyber Security Critical Systems Scoping Guidance" CAP 1849 (https://www.caa.co.uk/our-work/publications/documents/content/cap1849/).

Examples:

- Function: passenger booking; assets: application for passenger booking (software), website for passenger booking (software), check in kiosk (hardware), passenger database (data).
- Function: aeronautical data collection; assets: measuring equipment (hardware), processing software (software), measured data (data).

Different ways exist to inventory all the assets of the organisation. Beside the importance of having a clear and complete overview of the organisation's assets, the document should at least contain the information according to the following table.

Asset ID	A unique number or name for each asset.	
System name	The name of the system, tool, or equipment.	
Purpose of the asset	The function or role of the asset within your organisation.	
Type of asset	The kind of asset it is.	
	Hardware	Tangible ICT hardware used to support computing or networking operations. This includes devices you can physically handle (e.g. server, desktop, laptop, tablet, networking equipment, storage devices, IoT devices)
	Software	Locally installed programs that run on physical or virtual machines, typically requiring a license or installation package. Software that runs in a virtualised environment, often hosted on internal servers or virtual machines Software or services accessed via the internet, hosted and managed by external providers (SaaS).
	Information	Data, procedures, workflows, documentation,…
	Other	Use "Other" if you can't assign a pre-defined asset type. You may add a remark in the comment field.
Access	The people who can use or access the asset.	
	Employees only	Only internal staff or employees have access to the asset.
	External supplier / contractor	Access is granted to third-party vendors, service providers, or contractors.
	Public access	The asset can be accessed by the general public, with no authentication required.
	System only (no users)	The asset is used by other systems or services only; no direct human access.
	Other	Access does not fit the predefined categories; to be specified in the comment field.
Asset exposure	The environment or network scope through which the asset can be accessed.	
	Accessible from internet	The asset can be reached directly via the public internet, exposing it to external threats.
	Internal network only	The asset is accessible only within the organization's internal network, without public internet access.
	Isolated from network	The asset is physically or logically isolated and not connected to any network.
	Cloud-based	The asset is hosted in a cloud environment and accessed via the internet or private connections.
	Unknown	The exposure level of the asset is not currently known or documented.
Requirements in terms of C / I / A	Confidentiality (C): How important it is that data from the system stays private. Integrity (I): How important it is that data remains correct. Availability (A): How important it is that the system stays online.	
	High	
	Medium	
	Low	
Recovery time objective	The maximum acceptable downtime before the asset must be operational again.	
	Less than a day	
	Less than a week	
	Less than a month	
	More than a month	
	Not defined	

Business criticality	How essential the asset is to daily operations.	
	High	
	Medium	
	Low	
Impact on aviation safety	Indicate whether a loss of confidentiality, integrity, or availability of this asset could affect the safety of aviation operations, either directly or indirectly.	
	Yes	
	No	
Justification	If you select No on "Impact on Aviation Safety", please provide a justification.	
Comments	Additional notes, context, or clarifications about the asset.	
Last review date	When was the asset or its security last reviewed or updated.	

10. Appendix 3 – Risk assessment

10.1. Preamble

Aerodrome operators are invited to carefully read the definitions applicable to Part-IS, some concepts are new, namely the threats and the vulnerabilities, and there could be differences between those and the ones that are used in 139/2014. A safety risk refers to the predicted likelihood and severity of the consequences or outcomes of a hazard. Part-IS regulation mentions to use the term 'likelihood' instead of 'probability' to reflect a subjective analysis of the possibility of occurrence rather than a purely statistical assessment.

10.2. Risk assessment

Once the safety-critical assets are identified, the aerodrome is invited to describe all relevant and realistic scenarios that could affect these safety-critical assets. These scenarios should reflect actual threats and potential impacts within the aerodrome's operational context.

A single asset may be associated with multiple risk scenarios.

This risk assessment document should at least contain the following information.

Scenario ID	A unique number or name for each scenario.	
Asset ID	The corresponding Asset ID from the Asset Inventory.	
Threat source	The type of actor who could realistically cause harm to the asset.	
	Internal employee	A current staff member with legitimate access who may cause harm.
	Third-party	An external supplier, contractor, or service provider with authorised access.

	Former employee	Someone who previously worked for your organisation and may retain insider knowledge or access.
	Cybercriminal	An individual or group seeking financial or personal gain through unauthorised activities.
	Hacktivist	A politically or ideologically motivated attacker aiming to disrupt or expose.
	Opportunistic hacker	An unsophisticated attacker who exploits easily accessible vulnerabilities without targeting you specifically.
	Nation-state (advanced actor)	A highly skilled and well-resourced attacker linked to a government, often targeting critical infrastructure.
	Not sure	Used when the potential source of threat is unclear or unknown. Please provide further detail in the "Comments" column if this option is selected.
Motivation	The likely reason or objective behind a potential threat actor's actions.	
	Financial gain	The threat actor seeks to profit.
	Sabotage / Disruption	The goal is to cause intentional damage or interrupt operations, often to harm or make a statement.
	Espionage	The attacker is interested in gathering sensitive or strategic information, usually covertly.
	Automated threat (no specific motivation)	The attack is carried out by a bot or script scanning systems opportunistically, without human intent.
	Data stealing	The primary goal is to extract sensitive data (e.g. customer, employee, or operational data).
	Bandwidth abuse	The asset is exploited for computing or network resources (e.g. crypto mining, botnets).
	Other / unspecified	Please describe the specific situation in the "Comments" column to clarify.
Information Security Incident	A short description of what could go wrong.	
Impact	Describe the consequence of the information security incident on aviation safety.	
Likelihood	Estimate how likely this scenario is to occur.	
	Almost certain	The event is highly likely to occur; it happens frequently or has occurred before.
	Likely	The event is expected to occur in many circumstances.
	Possible	The event might occur at some time; there is a reasonable chance.
	Rare	The event is highly unlikely to occur but cannot be ruled out.
Severity	Assess the potential impact if the scenario were to occur.	
	Critical	Severe impact. High risk to life, potential for fatality, or major aviation incident.
	Major	Serious impact. Could compromise safety margins, cause significant disruptions, or result in injury.
	Moderate	Noticeable impact. May cause operational delays or require corrective actions, but no serious safety threat.
	Minor	Minimal impact. No significant effect on safety or operations.
Risk Level	Determine the overall risk by considering both likelihood and severity.	
	Unacceptable	The risk is high and generally not tolerable under normal circumstances.
	Conditionally acceptable	Requires implementation of additional compensating controls to ensure that there is no safety impact
	Acceptable	The risk is considered low and can be tolerated as is.
Justification	If you selected "Acceptable" in the "Risk Level" column, please provide a justification	
Comments	Additional notes, context, or clarifications about the risk scenario.	
Last Review	When was the asset or its security last reviewed or updated.	

11. Appendix 4 – Part-IS compliance self-assessment

The goal of the organisation's Part-IS compliance self-assessment is to assess whether the organisation has demonstrated that the foundation elements of the ISMS are established, and the organisation is ready to operate the ISMS. Most of the evidence related to this self assessment is expected to be part of the Information Security Management Manual (ISMM).

The assessment shall be completed in by the aerodrome operator in the form provided on the BCAA extranet under **Doc IS**. This form includes all requirements established by Part-IS, some elements related to the implementation of the ISMS could be stated as not compliant or not provided during the initial setup of the ISMS.

Part	Rule IS	Reference Number	Commision Reg	Compliance	Implementation plan	Contracted activities	AltMoC	Aerodrome Manual
IS.D.OR	Scope	IS.D.OR.100	(EU) 2022/1645					
IS.D.OR	Information security management system (ISMS)	IS.D.OR.200	(EU) 2022/1645					
IS.D.OR	Information security management system (ISMS)	AMC1 IS.D.OR.200(a)(1)	ED Decision 2023/009/R					
IS.D.OR	Information security management system (ISMS)	AMC1 IS.D.OR.200(a)(12)	ED Decision 2023/009/R					
IS.D.OR	Information security management system (ISMS)	AMC1 IS.D.OR.200(a)(13)	ED Decision 2023/009/R					
IS.D.OR	Information security management system (ISMS)	AMC1 IS.D.OR.200(c)	ED Decision 2023/009/R					
IS.D.OR	Information security management system (ISMS)	AMC1 IS.D.OR.200(e)	ED Decision 2023/009/R					
IS.D.OR	Information security risk assessment	IS.D.OR.205	(EU) 2022/1645					
IS.D.OR	Information security risk assessment	AMC1 IS.D.OR.205(a)	ED Decision 2023/009/R					
IS.D.OR	Information security risk assessment	AMC1 IS.D.OR.205(b)	ED Decision 2023/009/R					
IS.D.OR	Information security risk assessment	AMC1 IS.D.OR.205(c)	ED Decision 2023/009/R					
IS.D.OR	Information security risk assessment	AMC1 IS.D.OR.205(d)	ED Decision 2023/009/R					
IS.D.OR	Information security risk treatment	IS.D.OR.210	(EU) 2022/1645					

Part	Rule IS	Reference Number	Commision Reg	Compliance	Implementation plan	Contracted activities	AltMoC	Aerodrome Manual
IS.D.OR	Information security risk treatment	AMC1 IS.D.OR.210(a)	ED Decision 2023/009/R					
IS.D.OR	Information security internal reporting scheme	IS.D.OR.215	(EU) 2022/1645					
IS.D.OR	Information security internal reporting scheme	AMC1 IS.D.OR.215(a)&(b)	ED Decision 2023/009/R					
IS.D.OR	Information security incidents — detection, response and recovery	IS.D.OR.220	(EU) 2022/1645					
IS.D.OR	Information security incidents — detection, response and recovery	AMC1 IS.D.OR.220(a)	ED Decision 2023/009/R					
IS.D.OR	Information security incidents — detection, response and recovery	AMC1 IS.D.OR.220(b)	ED Decision 2023/009/R					
IS.D.OR	Information security incidents — detection, response and recovery	AMC1 IS.D.OR.220(c)	ED Decision 2023/009/R					
IS.D.OR	Response to findings notified by the competent authority	IS.D.OR.225	(EU) 2022/1645					
IS.D.OR	Response to findings notified by the competent authority	AMC1 IS.D.OR.225	ED Decision 2023/009/R					
IS.D.OR	Information security external reporting scheme	IS.D.OR.230	(EU) 2022/1645					
IS.D.OR	Information security external reporting scheme	AMC1 IS.D.OR.230(a)&(b)	ED Decision 2023/009/R					
IS.D.OR	Information security external reporting scheme	AMC1 IS.D.OR.230(c)	ED Decision 2023/009/R					
IS.D.OR	Contracting of information security management activities	IS.D.OR.235	(EU) 2022/1645					
IS.D.OR	Contracting of information security management activities	AMC1 IS.D.OR.235(a)	ED Decision 2023/009/R					

Part	Rule IS	Reference Number	Commision Reg	Compliance	Implementation plan	Contracted activities	AltMoC	Aerodrome Manual
IS.D.OR	Contracting of information security management activities	AMC1 IS.D.OR.235(b)	ED Decision 2023/009/R					
IS.D.OR	Personnel requirements	IS.D.OR.240	(EU) 2022/1645					
IS.D.OR	Personnel requirements	AMC1 IS.D.OR.240(a)(2)	ED Decision 2023/009/R					
IS.D.OR	Personnel requirements	AMC1 IS.D.OR.240(a)(3)	ED Decision 2023/009/R					
IS.D.OR	Personnel requirements	AMC1 IS.D.OR.240(b)	ED Decision 2023/009/R					
IS.D.OR	Personnel requirements	AMC1 IS.D.OR.240(d)	ED Decision 2023/009/R					
IS.D.OR	Personnel requirements	AMC1 IS.D.OR.240(f)	ED Decision 2023/009/R					
IS.D.OR	Personnel requirements	AMC1 IS.D.OR.240(g)	ED Decision 2023/009/R					
IS.D.OR	Personnel requirements	AMC1 IS.D.OR.240(h)	ED Decision 2023/009/R					
IS.D.OR	Personnel requirements	AMC1 IS.D.OR.240(i)	ED Decision 2023/009/R					
IS.D.OR	Record-keeping	IS.D.OR.245	(EU) 2022/1645					
IS.D.OR	Record-keeping	AMC1 IS.D.OR.245(a)(1)(vi)&(a)(5)	ED Decision 2023/009/R					
IS.D.OR	Record-keeping	AMC1 IS.D.OR.245(c)&(d)	ED Decision 2023/009/R					
IS.D.OR	Information security management manual (ISMM)	IS.D.OR.250	(EU) 2022/1645					
IS.D.OR	Changes to the information security management system	IS.D.OR.255	(EU) 2022/1645					
IS.D.OR	Changes to the information security management system	AMC1 IS.D.OR.255	ED Decision 2023/009/R					
IS.D.OR	Continuous improvement	IS.D.OR.260	(EU) 2022/1645					
IS.D.OR	Continuous improvement	AMC1 IS.D.OR.260	ED Decision 2023/009/R					
IS.D.OR	Continuous improvement	AMC1 IS.D.OR.260(a)	ED Decision 2023/009/R					
IS.D.OR	Continuous improvement	AMC1 IS.D.OR.260(b)	ED Decision 2023/009/R					