Derogation Guidance

Production Organisations

10.09.2025

Version: 1.0

Table of Contents

1. Abbreviations

ACG ..... Austro Control GmbH

AeMC ..... Aeromedical Centre

AMC ..... Acceptable Means of Compliance

ANSP ..... Air Navigation Service Provider

BITD ..... Basic Instrument Training Device

EASA ..... European Aviation Safety Agency

FSTD ..... Flight Simulation Training Device

FTD ..... Flight Training Device

CAMO ..... Continuing Airworthiness Management Organisation

CAT ..... Commercial Air Transport

CMPA ..... Complex Motor Powered Aircraft

DOA ..... Design Organisation Approval

ELA ..... European Light Aircraft

FNPT ..... Flight Navigation Procedures Trainer

GM ..... Guidance Material

ISMS ..... Information Security Management System

IT ..... Information Technology

MOA ..... Maintenance Organisation Approval

MTOM ..... Maximum Take-Off Mass

OT ..... Operational Technology

POA ..... Production Organisation Approval

SMS ..... Safety Management System

2. Purpose of this Guidance Material

This document is intended to support organizations in the identification and assessment of potential derogation requests in accordance with IS.I/D.OR.200(e). It outlines Austro Control's interpretation and application of the relevant regulatory requirements and serves as a supplement to the EASA Part-IS Guidance Material, as presented in the *Easy Access Rules for Information Security*, along with other applicable guidance documents.

Furthermore, it provides detailed instructions for completing the derogation application and offers guidance on the preparation and submission of the required supporting documentation.

3. Exceptions for the applicability of Part-IS

If the scope of work of an organisation aligns with the exceptions stated in the table below, most Part-IS requirements are not applicable for the organisation and no further actions need to be considered in terms of compliance. Therefore, a derogation is not necessary.

Domain	Exceptions
Production and Design Organisations (Part-21)	• Solely involved in the production of ELA 2 aircraft This only applies to organisations that produce complete aircraft. Other organisations that produce other products or parts (e.g. engines, propellers, landing gears, pumps, etc.) cannot be excluded from Part-IS, even if they can demonstrate that their products or parts can only be installed in ELA2 aircraft.

Figure 1: Applicability based on MTOM

IS.I/D.OR.200(e) opens the opportunity to organisations to ask for an approval for an derogation to implement most of the requirements of Part IS, if it demonstrates that its activities, facilities and resources, as well as the services it operates, provides, receives and maintains, do not pose any information security risks with a potential impact on aviation safety neither to itself nor to other organisations.

In most cases, the derogation is fully applicable to the specified requirements. However, in certain instances, the requirement may remain either fully or partially in effect.

IS.I/D.OR.200(a)(13): The organisation must ensure the confidentiality of any information received from other entities, in accordance with its sensitivity level, and without prejudice to any applicable incident reporting obligations.

IS.I/D.OR.205(d): It is recognized that the business environment in which aviation organizations operate is dynamic and subject to continuous evolution. Factors such as technological advancements, regulatory developments and emerging cybersecurity threats may significantly alter operational conditions over time. Consequently, the implementation and oversight of Part-IS should remain flexible and responsive to these changes, ensuring that information security measures remain effective, proportionate, and aligned with the organization's current risk landscape. Therefore, a risk assessment process identifying potential information security risks will still need to be applied, as necessary.

IS.I/D.OR.230: the reporting requirements laid down in Commission Regulation (EU) No 376/2014 still apply.

IS.I/D.OR.240(a)(3): the Accountable Manager must be able to demonstrate a basic understanding for the requirements of regulations 2023/203 or 2022/1645

4. Derogation

4.1. Recognition of Derogation Possibility

Austro Control (ACG) acknowledges that organisations may seek approval to refrain from implementing certain requirements of Part-IS, in accordance with IS.I/D.OR.200(e). ACG is committed to supporting such applications wherever feasible and appropriate.

4.2. Derogation Evaluation and Approval

An organisation may be granted approval by ACG to refrain from applying the requirements specified in points IS.I.OR.200 (a) to (d), as well as the related provisions outlined in IS.I/D.OR.205 to IS.I/D.OR.260, provided it can demonstrate— to the satisfaction of ACG— that its activities, facilities, resources, and the services it operates, provides, receives, or maintains do not present an information security risk with potential implications for aviation safety, either to itself or to other organisations. Such an approval is considered a derogation.

4.3.Risk Assessment Requirement

In all cases, the approval granted by ACG is contingent upon a documented information security risk assessment. This assessment should be conducted either by the organisation itself or by a qualified third party, in accordance with the provisions of IS.I/D.OR.205, and is subject to review and approval by ACG.

The risk assessment may be performed using the organisation's existing risk assessment procedures, provided they meet the necessary standards. Any identified risks should be recorded and continuously monitored within the organisation's risk register, as an integral part of its Safety Management System (SMS).

The risk assessment according to IS.I/D.OR.205 of an organisation builds the foundation of the assessment, whether ACG denies or grants a request. In addition to the risk assessment, other considerations are also taken into account.

For example:

High level consideration describing the exposure to the aviation landscape:

- The position of the organisation within the aviation functional chain, and
- its level of contribution to safety consequences.

Detailed consideration about processed or produced safety related information:

- The services the organisation provides and receives incl. their interfaces
- The processes the organisation has established to provide and receive the services

4.4.Important Note on Derogation Validity

Organisations are advised to remain vigilant and, at a minimum, reassess their exposure to cybersecurity threats whenever there is a change affecting their management system. The change procedure crediting indirect approval shall cover this issue.

The continued validity of an approved derogation is subject to review by ACG as part of the applicable oversight audit cycle. Additionally, any changes to be approved by ACG will trigger a reassessment of the derogation's relevance and applicability.

4.5.Assessment Criteria for Derogation Applications

To support organisations in evaluating the viability of their derogation requests, EASA has established three core criteria that serve as indicators for a "right-sized-ISMS".

Since there is no clear distinction between complex and non-complex organisations, when assessing an organisation's complexity in terms of information security, the assessment should consider each of the following elements separately. Each element, on its own, can influence certain aspects of a proportionate ISMS implementation:

- **Where the organisation is placed in the functional chain** and the number and safety relevance of the interfacing organisations/stakeholders.
- The **complexity of the organisational structure and hierarchies** (e.g. number of staff, departments, hierarchical layers, etc)
- The **complexity of the information and communication technology systems and data** used by the organisation and their connection to external parties.

If an assessment based on these criteria will result in "simple" in all three criteria, but specifically in the first criteria, the organisation falling within the scope of Part-IS is, in principle, could be eligible to apply for a derogation, ACG will conduct an initial triage of applications based on these criteria and the conditions outlined below, prior to undertaking a detailed assessment.

It is important to emphasise that the conditions and justifications outlined below do not constitute automatic grounds for either approval or rejection of a derogation request. Each application submitted by an organisation will be assessed on a case-by-case basis.

Criteria of possible derogation as a production organization:

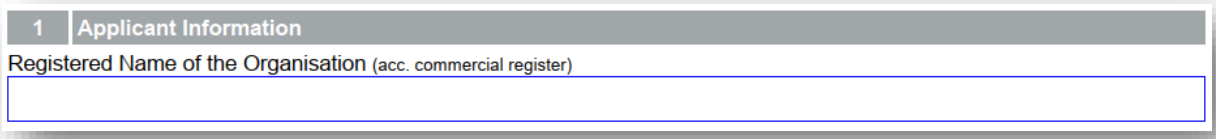
- Production of parts that are not part of the primary structure and do not provide safety-related functions: carpets, upholstery, belts, interior parts
- Production of parts that can be verified during the final inspection by measurement for complete compliance with the design data: Mechanical parts that have been machined only, Tied wire harnesses
- Production of parts that do not use IT-supported processes: manual welds, manually sewn belts
- Use of the "ELA2 applicability": The organisation is mainly producing for ELA2 aircraft and similar parts for related non-ELA2 aircraft by using the same processes and infrastructure

5. Application Form – guidance and explanations

When completing the ACG application form (FO_LFA_ALG_007_EN_v1.0), the organisation should provide the following information:

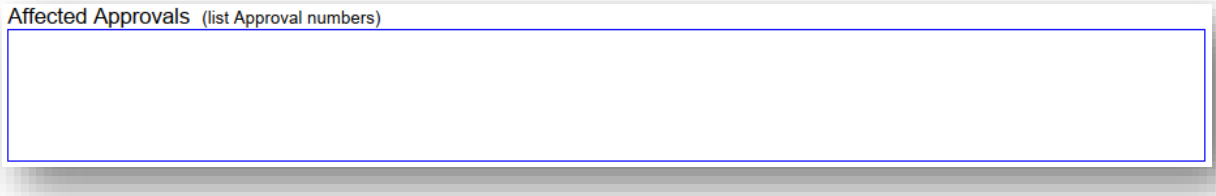
5.1. **Block 1:** Applicant Information

5.1.1. Registered name of the organisation



Self-explanatory (name of the organisation according to the commercial register ("Firmenbuch")).

5.1.2. Affected approvals



List all the approvals, as listed on the affected approval certificate(s), for which the derogation is sought, e.g.:

CAMO: AT.CAMO.194,

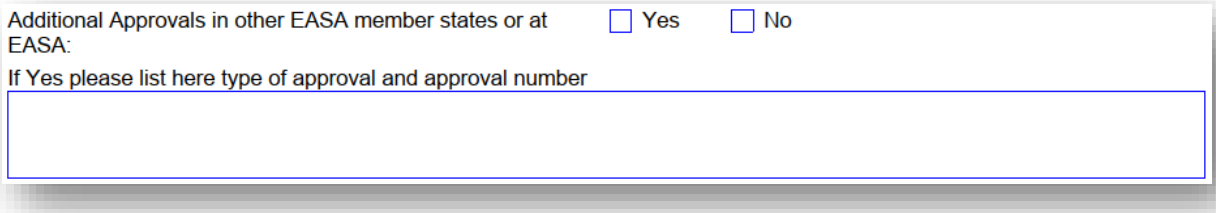
AOC: A-194,

Approved Training Organisation: AT.ATO.199

FSTD: AT-1A-1099,

Part-145 organisation: AT.145.099

Production organisation: AT.21G.097



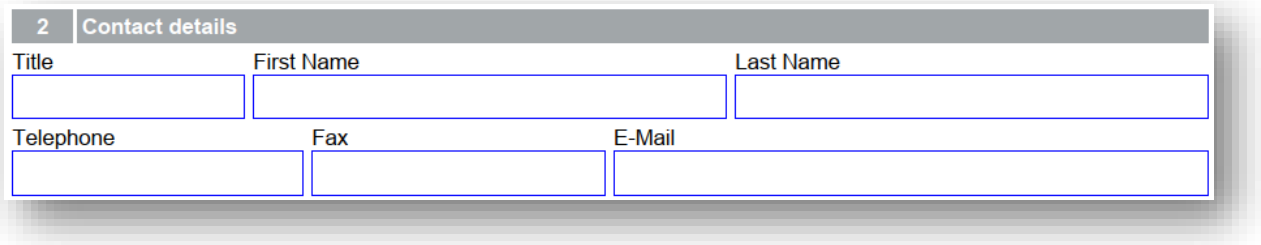
Coordination with Competent Authorities

Organisations holding multiple approvals in various EASA member states should inform all relevant Competent Authorities when submitting a derogation request. This includes notifying EASA when it acts as the Competent Authority. Such communication enables coordination among authorities, where deemed necessary.

Furthermore, the Competent Authority responsible for assessing the derogation may, at its discretion, inform EASA of the outcome of the assessment.

Where applicable, the organisation should list the affected approval references—such as *EASA.21G.0987* or *EASA.21J.0898* for EASA-issued approvals — or provide the relevant national approval reference number issued by the respective Member State.

5.2. **Block 2:** Contact Details



The organisation should assign and indicate a point of contact for further enquiries. This should be a person having the necessary competencies with regards to the information provided in the application.

5.3. **Block 3:** Exemption Request

As per IS.I/D.OR.200(e), any grant of approval for a derogation shall be based on a documented information security risk assessment carried out by the applicant organisation or an assigned third party. In accordance with IS.I/D.OR.205, this information security risk assessment shall identify the information security risks which may have a potential impact on aviation safety, neither to itself, nor to other organisations.

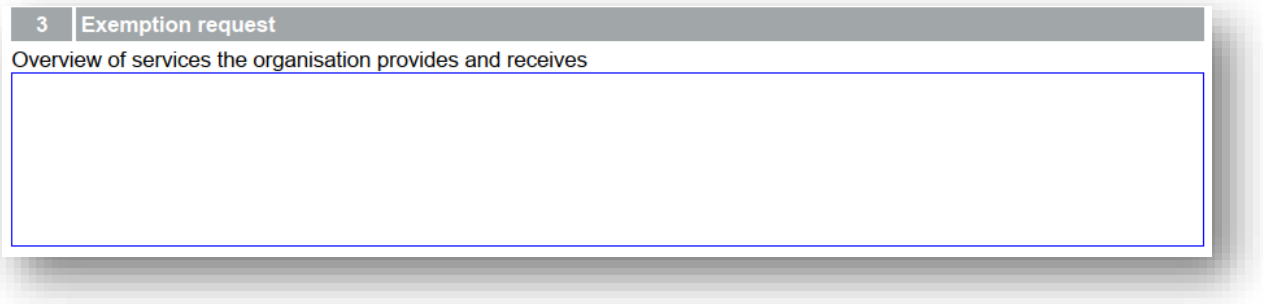
The risk assessment is expected to provide explanations for the exclusion of all elements from the scope of the ISMS. It is up to ACG to determine whether this assessment is deemed satisfactory for a derogation to be granted. Therefore, it is crucial to provide sufficient information for analysis and assessment:

- Is the documentation sufficient for a proper analysis and assessment?
- Is the repository of digital systems, data flows and processes comprehensive?
- Is the information security risk assessment conducted in accordance with the company's methodology?
- Was the information security risk assessment performed with the appropriate diligence?
- Were the relevant stakeholders involved in the information security risk assessment process?

- Was the information security risk assessment performed by people with sufficient expertise in information security and aviation safety?
- Has the organisation assigned and indicated a point of contact for enquiries?

Note: Organisations that would like to have the risk assessment performed by a third party should consider the requirements of IS.I.OR.235 and the related AMC.

5.3.1. Overview of the services the organisation provides and receives



The organization should clearly understand its aviation activities, services, related processes, and information systems. It should also know how data flows and information are exchanged, as this defines the scope of the Information Security Management System (ISMS) and the boundaries for risk assessment.

To support this, the organization should document the resources and dependencies—such as computing, networking, and third-party services—that could impact the security and safety of its operations within the risk assessment scope:

(a) illustrate (e.g. through a functional diagram) the relationships of logical and physical paths connecting the different parts involved;
(b) clearly identify all assets (i.e. hardware, software, network and computing resources) that will be used in the exchange;
(c) identify all functions, activities and processes, including their respective information and data, which will be created, transmitted, processed, received and stored, and associate those with the responsible party which provides or performs those functions, activities and processes;
(d) determine for these paths, constituting the so-called functional chains (see Cover Regulations, GM1 Article 3 — Definitions), the role of the interfacing party as a producer, processor, dispatcher or consumer of the information or data involved;
(e) determine whether one interfacing party acts as an originator or receiver of a flow across such path.

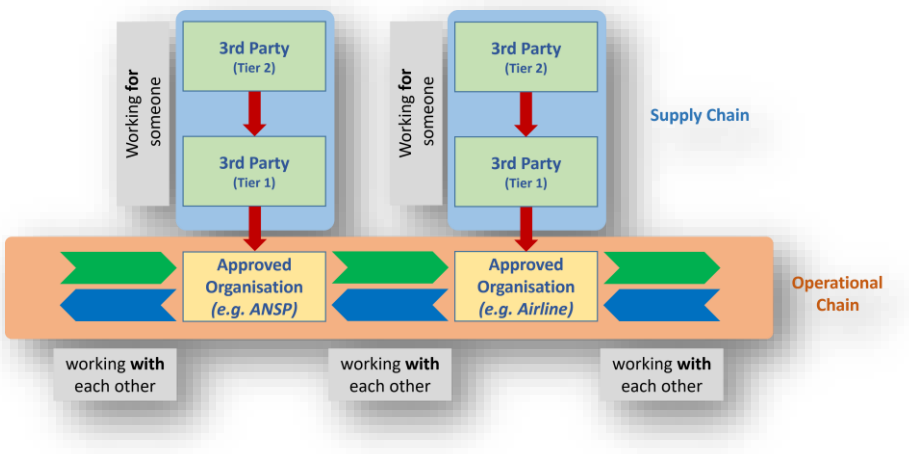


Figure 2 The Functional Chain Approach

5.3.2. Architecture overview of information systems used for business operation

Architecture overview of information systems used for business operation

An "**Architecture overview of information systems used for business operation**" is a high-level map or description of all the key IT systems and how they work together to support the organization's daily activities. It helps people understand what systems exist, what they do, and how they connect. The purpose of this overview is to help identify:

- Critical assets and dependencies
- Potential vulnerabilities
- Scope for risk assessment and mitigation

What It Typically Includes:

Core Business Systems
These are the main tools used to run the business, such as ERP (Enterprise Resource Planning), CRM (Customer Relationship Management), HR systems as well as key systems and applications used in operations, such as flight planning, maintenance tracking, passenger services, air traffic communication

Supporting Systems
These help the core systems function, like Databases, File storage, Email and communication tools and Authentication and access control systems

Interfaces and Connections
Data flows between systems, showing how information is exchanged internally and externally

Security Boundaries (Layers)
showing where protections like firewalls, access controls, and monitoring are applied

Infrastructure components
Such as servers, networks, databases, and cloud services

5.3.3. Methodology used to perform the information security risk assessment

Methodology used to perform the information security risk assessment

It is recommended to use the risks assessment methodology already established by the organisation´s Safety Management System, enhanced with the information security aspects.

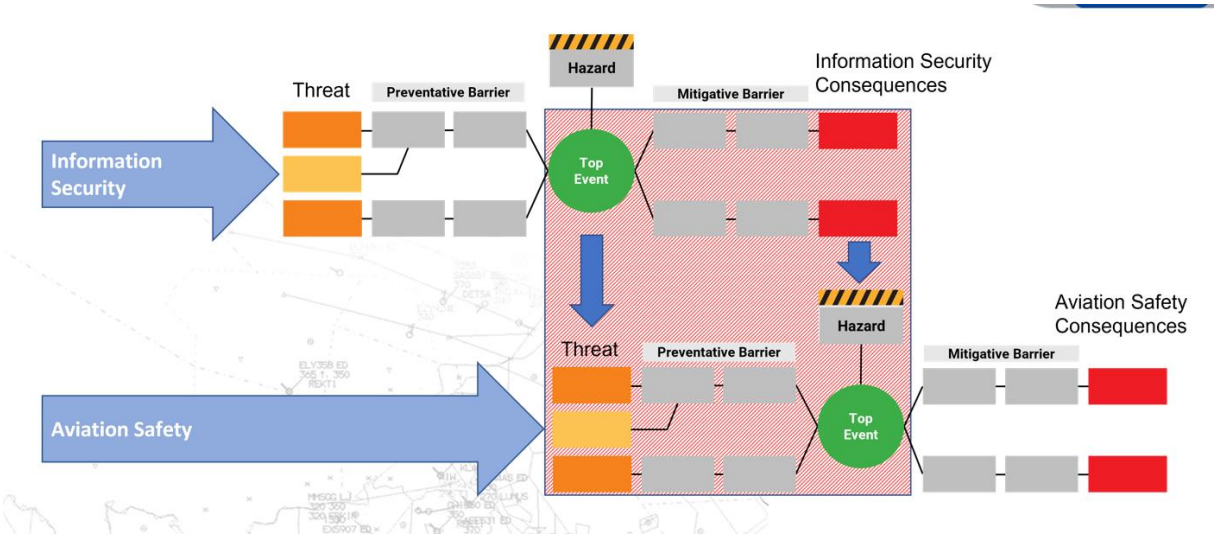


Figure 3 Relationship between IS-Risk Assessment and Safety Risk Assessment

The "**methodology used to perform the information security risk assessment**" refers to the structured approach an aviation organization follows to identify, evaluate, and manage cybersecurity risks that could impact aviation safety. If ever possible, the already established risk

assessment methodology as a mandatory part of the SMS of the organisation should be used to address information security risks.

The common elements of the Risk Assessment Methodology expected are as follows:

Asset Identification
What are you protecting? (e.g., servers, data, software)

Threat Identification
What could harm those assets? (e.g., cyberattacks, human error)

Vulnerability Assessment
What weaknesses exist that threats could exploit?

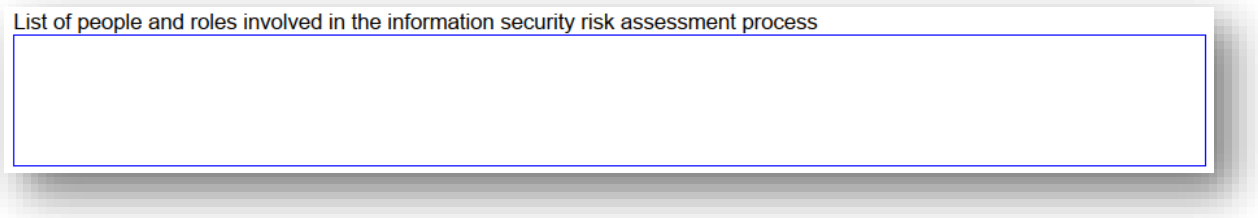
Impact
Describe the consequence of the Information Security Incident on aviation safety

Risk Analysis
Combine threat + vulnerability + impact to estimate the risk level.

Risk Treatment
Choose how to handle each risk, e.g.:

> **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

5.3.4. List of people / roles involved in the information security risk assessment process



The **"list of people and roles involved in the information security risk assessment process"** refers to the identification and documentation of all individuals and their responsibilities in conducting, supporting, and overseeing the risk assessment. Here's what ACG typically expects to be included:

Accountable Manager

- Approves the risk assessment methodology and outcomes.
- Ensures resources and support for mitigation measures.

Safety Manager

- Ensures integration of cybersecurity risks with aviation safety risk management.
- Supports alignment with the Safety Management System (SMS).

Compliance Monitoring Manager

- Ensures regulatory and internal compliance.
- Support audits, verify assessment standards.

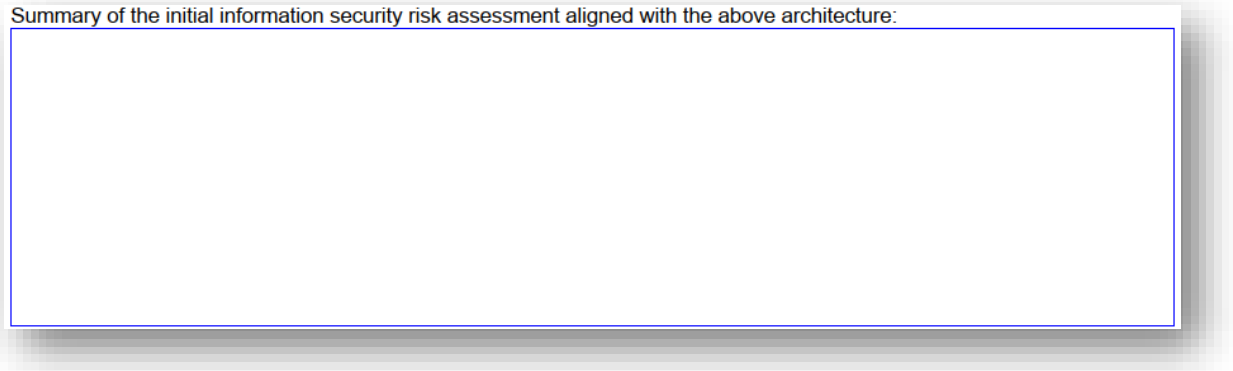
Risk Assessment Team Members

- Subject matter experts from IT, operations, safety, and compliance.
- Contribute technical and operational insights.
- Help identify assets, threats, and vulnerabilities.

External Consultants or Service Providers (if applicable)

- May assist with specialized assessments or tools.
- Should be clearly identified and their roles defined.

5.3.5. Summary of the initial information security risk assessment



The **"summary of the initial information security risk assessment, aligned with the architecture overview of information systems used for business operations"**, should provide a clear and brief picture of the organization's cybersecurity status, based on how its information systems are set up for business operations. It helps demonstrate that the organization has thoroughly assessed its exposure to cybersecurity risks and can justify why a full ISMS may not be necessary.

The summary should include:

1. High-Level Risk Assessment Summary

- A concise overview of the information security risks identified.
- Focus on risks that could impact aviation safety, directly or indirectly.
- Explanation of why these risks are low or manageable without a full ISMS.

2. Alignment with Architecture Overview

- Reference to the architecture of information systems used in business operations.
- Show how the systems are isolated, limited in scope, or not safety-critical.
- Demonstrate that data flows, interfaces, and dependencies do not introduce significant cybersecurity risks.

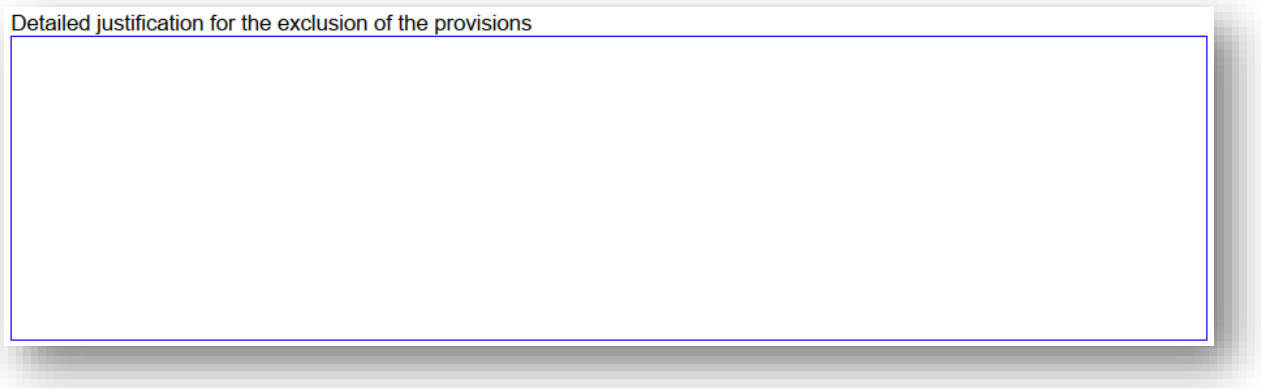
3. Organizational Role in the Aviation Ecosystem

- Describe the organization's position in the aviation functional chain.
- Clarify whether it contributes to safety-critical functions (e.g., flight control, avionics, navigation).
- If not, explain how its role is limited to non-critical components (e.g., cabin interiors, documentation).

4. Justification for Derogation

- Clearly state why the organization believes it qualifies for a derogation.
- Support this with evidence from the risk assessment and system architecture.
- Mention any mitigating measures already in place (e.g., basic cybersecurity controls, supplier vetting).

5.3.6. Detailed justification for the exclusion of the provisions



The "**detailed justification for the exclusion of the provisions**" should clearly explain why the organization believes it does not need to fully comply with the ISMS (Information Security Management System) requirements.

It should include the following elements:

1. Explanation of Low or No Risk to Aviation Safety

- Demonstrate that the organization's activities do not pose a cybersecurity risk that could impact aviation safety.
- This includes showing that the organization:
- Does not handle safety-critical systems (e.g., avionics, navigation, flight control).

- Designs or produces non-critical components (e.g., cabin interiors, carpets).
- Has limited or no digital interfaces with safety-relevant systems.

2. Results of an Initial Risk Assessment

- Provide a summary of the initial information security risk assessment.
- Show that the identified risks are minimal or well-controlled.
- Align this with the architecture overview of the organization's information systems.

3. Scope and Boundaries of Activities

- Clearly define the scope of the organization's operations.
- Explain how these operations are isolated from safety-critical systems or do not contribute to aviation safety functions.

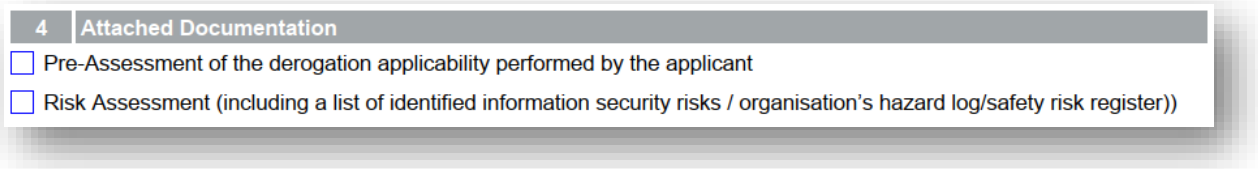
4. Supporting Evidence

- Include documentation such as:
- System architecture diagrams
- Asset inventories
- Data flow maps
- Contracts showing limited service scope

5. Commitment to Reassessment

- Acknowledge that the derogation is temporary.
- Commit to reassessing cybersecurity exposure if the scope of work changes.

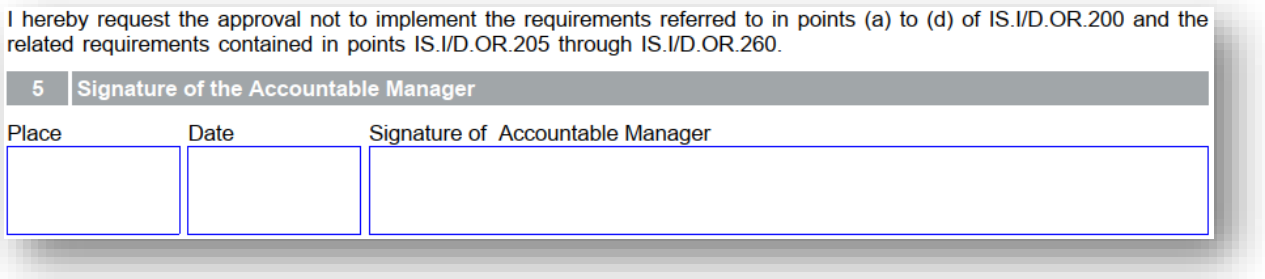
5.4. **Block 4:** Attached Documentation



The objective is to obtain preliminary information about the organisations information security risk profile. To enhance efficiency, organisations should conduct a preliminary self-assessment ("pre-assessment") prior to the detailed evaluation by ACG. The information provided in the application form (FO_LFA_ALG_007_EN_v1.0) serves as an initial, high-level assessment, enabling ACG to determine whether a derogation request warrants further detailed review. No

fees will be charged in cases where the derogation request is deemed unlikely to result in a positive outcome.

5.5. **Block 5:** Signature of the Accountable Manager



I hereby request the approval not to implement the requirements referred to in points (a) to (d) of IS.I/D.OR.200 and the related requirements contained in points IS.I/D.OR.205 through IS.I/D.OR.260.

5	Signature of the Accountable Manager	
Place	Date	Signature of Accountable Manager

Self explanatory.

6. Fees

ACGV TP97: Alle sonstigen Amtshandlungen infolge eines Parteienansuchens, die nicht unter eine andere Tarifpost fallen, zuzüglich des Aufwandes gemäß TP 92.

7. Online Resources and References

- EASA FAQs
- EASA Rules
- Acceptable Means of Compliance (AMC) und Guidance Material (GM)
- EASA Easy Access Rule
- ICAO page on cyber security
- Guidelines for ISO/IEC 27001:2022 conforming organisations on how to show compliance with Part-IS
- Implementation guidelines for Part-IS - IS.I/D.OR.200 (e)
- Part-IS Oversight Approach Guidelines
- Application of the European Cybersecurity Skills Framework to Aviation
- Part-IS Compliance Assessment Tool