Guidelines

Implementation guidelines for Part-IS* - IS.I/D.OR.200 (e)

Part-IS TF G-02

July 2024

"This document has been developed by the Part-IS Implementation Task Force, a collaborative effort of EASA States civil aviation authorities. The Task Force has worked with great care to produce a comprehensive set of guidelines aimed at ensuring a harmonised implementation of Part-IS across Member States. This initiative is part of the ongoing commitment to maintain high standards of aviation safety throughout the European Union."

* A set of rules contained in Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 and in Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 laying down requirements for the management of information security risks with a potential impact on aviation safety for aviation organisations and authorities across the entire aviation domain.

Guidelines

Implementation guidelines for Part-IS - IS.I/D.OR.200 (e)

Document ref.	Status	Date
Part-IS TF G-02	Issued	15/07/2024
Contact name and address for enquiries:	cybersec@easa.europa.eu European Aviation Safety Agency Cybersecurity and Emerging Risks Section Postfach 10 12 53 50452 Köln Germany	
Information on EASA is available at:	www.easa.europa.eu	
This document is published on the basis of Article 1(3)(f) of Regulation (EU) 2018/1139 which states that the objectives of that Regulation shall be achieved by, inter alia: 'the uniform implementation of all necessary acts by the national competent authorities and the Agency, within their respective areas of responsibility;'. Of relevance is one of the objectives enshrined in Article 1(2), namely to 'promote cost-efficiency, by, inter alia, avoiding duplication, and promoting effectiveness in regulatory, certification and oversight processes as well as an efficient use of related resources at Union and national level;' This document is also published in conjunction with Art. 5(3) of Regulation (EU) No 628/2013: "The Agency shall rovide competent authorities of Member States with relevant information to support the uniform implementation of the applicable requirements."		

Authorisation :			
	Name	Signature	Date
Prepared	N/A	N/A	-
Reviewed	N/A	Adopted by Part-IS Task Force	15/07/2024

Table of Contents

Table of Figures

Table of Tables

1 Executive summary

This implementation guidance aims to harmonise the process for organisations to apply for derogations and their assessment and approval by Competent Authorities in all Member States, while ensuring continuous monitoring to maintain the validity of the supporting evidence.

A conservative approach to approval, coordination between authorities and pre-assessment using tailored documentation is recommended. The assessment criteria include the organisation's exposure to the aviation landscape, safety contribution and processes, taking into account factors such as scope of work, complexity, safety impact, criticality, cross-border activities and SMS maturity.

2 Introduction

The purpose of this implementation guideline is to harmonise the process of derogation requests by organisations and the assessment and approval of same by Competent Authorities, across the Member States. This includes the ongoing monitoring of derogation approvals issued, to ensure that the supporting evidence on which they were granted remains valid.
A harmonised approach by both the organisation and the Competent Authority, to the management of derogation requests and subsequent monitoring of any approvals granted, is important to ensure uniform application across Member States. This is especially important in the case where an organisation operates across National borders and may have to interface with multiple Competent Authorities.

3 General principles

- In general, the Competent Authority should adopt a conservative approach within its process for assessing derogation requests and determining if an approval should be granted. If in doubt, the Competent Authority should refrain from granting a derogation. Once a derogation approval is issued, the Competent Authority needs to ensure that the validity of the derogation and the basis on which it was granted, is reviewed on a regular basis and whenever it is notified of any implemented changes in the scope of work of the organisation.
- An entity holding multiple approvals should inform the different Competent Authorities (incl. EASA when acting as a Competent Authority), in the case where they are seeking a derogation in a member state. This allows the Competent Authorities to coordinate if deemed necessary. In addition, the Competent Authority assessing the derogation may decide to inform the EASA about the results of these assessments.
- For efficiency reasons, it is recommended to pre-assess a request for derogation before a detailed assessment is conducted by the Competent Authority. Therefore, a questionnaire, self-assessment template, or similar specific tailored document for the intended approval type should be issued by the Competent Authority.
- 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 below criteria should be considered in the evaluation of the derogation request and accompanying information security risk assessment.

- High level consideration describing the exposure to the aviation landscape:
  - The position of the organization 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

Therefore, in terms of evidence and information, the following should be considered:

1. Scope of work
2. Size and complexity of the organisation
3. Potential (additional) safety impact caused by information security incidents
4. Criticality of the organisation for the civil aviation landscape within the Member State
5. Cross-border activities of the organisation, if applicable
6. Maturity of the organisation’s safety management system

Changes in the scope of work and of any activities of the organisation which may impact the derogation approval, shall be notified to the Competent Authority, as specified in the implementing rule as an inherent part of the change management procedure approved by the competent authority. Such a notification acts as a trigger for a review and subsequent re-evaluation of the validity of the approved derogation by the Competent Authority.

4 Expectations and recommendation of the Competent Authority

Once a derogation approval has been granted, the Competent Authority expects the organisation to undertake the following on a continual basis.

- To comply with all provisions of the rule which are not exempted (e.g. OR.200 (a) (13)).
- To continually monitor any changes in the organisation ‘s scope of work and identify those which may have a potential impact on the documented information, which supports the derogation approval. Where such changes are identified, the organisation should ensure that they are brought to the attention of the Competent Authority without delay and notified in accordance with the applicable implementing rule.
- The accountable manager of the organisation can demonstrate an understanding of the derogation process and the terms on which the approval has been granted.
- To implement basic protection against information security risks according to industry best practices.
- To consult the respective National cyber security body for additional guidance.

5 Application for derogation

The Competent Authority should establish an official derogation request application form template and make it available to all organisations. This will ensure that a consistent approach is followed by organisations when submitting a request for a derogation. The application form will need to be completed and signed off by the applicant organisation's accountable manager and sent to the respective Competent Authority for review and consideration.
The content within that form serves as preliminary and high-level assessment for the Competent Authority before it further requests more details.

The application form should contain preliminary information used for a pre-assessment

- Company information and contact information
- Affected approval(s)
- Detailed justification for the exclusion of the provisions
- Overview of services the organisations provides and receives
- Architecture overview of information systems used for business operation
- Summary of the initial information security risk assessment aligned with the above architecture
- Methodology used to perform the information security risk assessment
- List of people and roles involved in the information security risk assessment process
- Date and signature

6 Assessment of the derogation application

As per OR.200(e), the competent authority to grant 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 OR.205(c), this information security risk assessment shall identify the information security risks which may have a potential impact on aviation safety.
To this end, the organisation's information security risk assessment and other supporting documentation should be subject to review by a panel with multidisciplinary expertise, in particular:

- Understanding of the organisation's operational domain (the involvement of a domain specific inspector is recommended)
- Information security expertise
- Aviation safety process expertise

Items to be assessed

- ✓ 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?

7 Provisions to be compliant with, regardless of approved derogation

IS.I.OR.200 (a)(13)
The organisation protects, without prejudice to applicable incident reporting requirements, the confidentiality of any information it may have received from other organisations, according to its level of sensitivity.

The Competent Authority should verify that the organisation

- ✓ has adequate measures in place to protect the confidentiality of information at rest and in transit
- ✓ has established a data classification scheme
- ✓ has established appropriate access control measures to ensure an effective "need-to-know" principle

See also below Table 1 for more details on the partial applicability of some of the requirements in spite of the derogation.

8 Process example

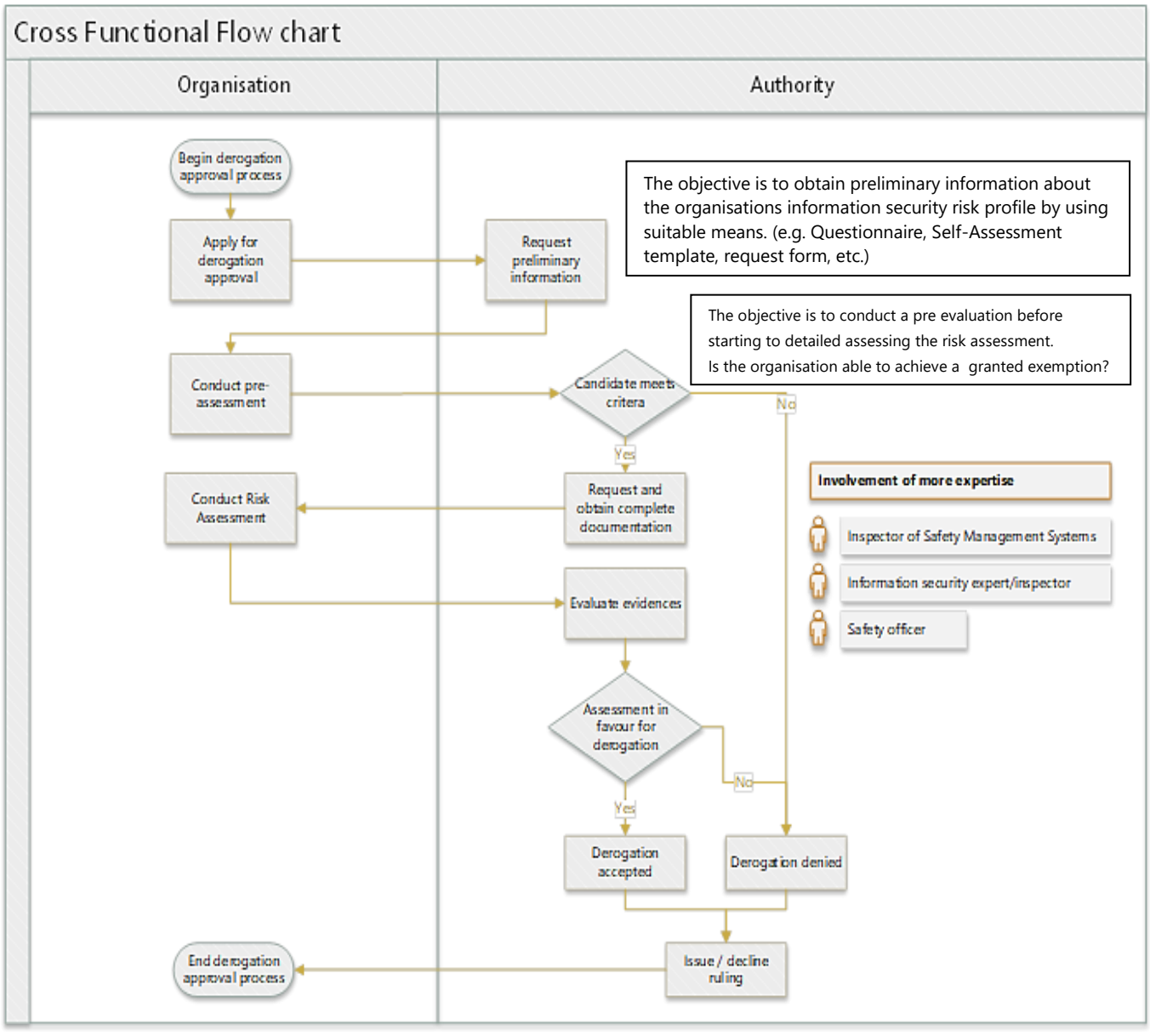

Figure 1 – Cross functional flow chart of the derogation approval process

Appendix I – Detailed list of the requirements affected by the derogation

Table 1 below gives a detailed list of the Part IS requirements affected by the derogation. For most of the requirements the derogation applies in full (green cell in the table below), in a few cases the requirement still applies (white cell) or partially applies (yellow cell).

Table 1 – List of requirements that are released from implementation if a derogation is granted

Provision of the regulation **green:** full derogation **yellow:** partial derogation **white**: no derogation	**Content**	**Remark**
IS.I.OR.200 (a)	Implementation of an ISMS	
IS.I.OR.200 (a) (1)	Information security policy	
IS.I.OR.200 (a) (2)	Identification and review of information security risks	
IS.I.OR.200 (a) (3)	Definition and implementation of risk treatment	
IS.I.OR.200 (a) (4)	Internal reporting scheme	
IS.I.OR.200 (a) (5)	Implementation of measures for detection of information security events and incidents	
IS.I.OR.200 (a) (6)	Implementation of measures as an immediate reaction to a vulnerability or information security incident	
IS.I.OR.200 (a) (7)	Actions required to address findings notified by the competent authority	
IS.I.OR.200 (a) (8)	Implementation of an external reporting scheme	
IS.I.OR.200 (a) (9)	Maintaining compliance to the requirements when contracting information security management activities (IS.I.OR.235)	
IS.I.OR.200 (a) (10)	Maintaining compliance regarding personnel requirements	
IS.I.OR.200 (a) (11)	Record keeping	
IS.I.OR.200 (a) (12)	Compliance monitoring	
IS.I.OR.200 (a) (13)	Protect confidentiality of information received from other organisations	This requirement should not be limited to only protect the received information. When transmitting information with confidential nature, the organisation needs to have secure means in place as well.

Provision of the regulation green: full derogation yellow: partial derogation white: no derogation	Content	Remark
IS.I.OR.200 (b)	Continuous improvement	
IS.I.OR.200 (c)(d)	Documentation of key processes, procedures and roles & responsibilities.	
IS.I.OR.205	Information security risk assessment	At least IS.I.OR205 (d) should still be applicable. Business environment can and will change over time.
IS.I.OR.210	Information security risk treatment	
IS.I.OR.215	Internal reporting regarding information security	
IS.I.OR.220	Detect information security events and incidents. Measures for response and recovery.	
IS.I.OR.225	Obligation to findings notified by the CA	
IS.I.OR.230	Report incidents to the CA	
IS.I.OR.235	Manage risks for contracted activities	
IS.I.OR.240	Additional personnel requirements	At least IS.I.OR.240 (3) should still be applicable. Someone needs to have an understanding of the rule.
IS.I.OR.245	Record-keeping regarding information security	
IS.I.OR.250	Information Security Management Manual (ISMM)	
IS.I.OR.255	Seek for approval upon changes	
IS.I.OR.260	Continuous improvement	

Appendix II –IS.I.OR.200 (e) requirement and related AMC and GM

IS.I.OR.200 Information security management system (ISMS)

(e) Without prejudice to the obligation to comply with the reporting requirements laid down in Regulation (EU) No 376/2014 and the requirements laid down in point IS.I.OR.200 (a)(13), the organisation **may be approved by the competent authority not to implement the requirements** referred to in points (a) to (d) and the related requirements contained in points IS.I.OR.205 through IS.I.OR.260, **if it demonstrates to the satisfaction of that authority** 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. **The approval shall be based on a documented information security risk assessment** carried out by the organisation or a third party in accordance with point IS.I.OR.205 and reviewed and approved by its competent authority.

The continued validity of that approval will be reviewed by the competent authority following the applicable oversight audit cycle and whenever changes are implemented in the scope of work of the organisation.

AMC1 IS.I.OR.200(e) Information security management system (ISMS)

DEROGATION

Organisations should follow the directions provided in AMC1 IS.I.OR.205(a) and AMC1 IS.I.OR.205(b) to perform a documented information security risk assessment to seek the approval by the competent authority of a derogation under point IS.I.OR.200(e). In order to justify the grounds for a derogation, the risk assessment is expected to provide explanations for the exclusion of all elements from the scope of the ISMS. It is up to the authority to determine whether this assessment is deemed satisfactory for a derogation to be granted.

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.

GM1 IS.I.OR.200(e) Information security management system (ISMS)

Any organisation that believes that it does not pose any information security risk with a potential impact on aviation safety, either to itself or to other organisations, may consider requesting an approval for a derogation by the competent authority following the procedure outlined in AMC1 IS.I.OR.200(e).

Some examples of organisations that may consider asking for a derogation might include:

- An air operator that performs non-high-risk commercial specialised operations (SPO) with non-complex aircraft, if the nature of the operations justifies the grounds for a derogation.
- An air operator that operates ELA2 aircraft as defined in Article 1(2)(j) of Regulation (EU) No 748/2012 with the exception of one aircraft that is operated in predefined operational conditions or under certain operational limitations.
- A maintenance organisation approved under Part-145 dealing only with maintenance of components or maintenance activities that do not contribute to ensuring the structural integrity of the aircraft nor any major safety-related functionalities — for instance, undertaking activities such as washing, removing coatings, painting, etc.

The aforementioned examples are not exhaustive and are only indicative of potential scenarios that might provide an initial basis for the preparation of an information security risk assessment that justifies the exclusion of all elements of an organisation from the scope of the ISMS.