SOFEMA
AVIATION SERVICES

Sofema Aviation Services Considers Grounds for Requesting a Derogation under Part-IS (EASA 2023_203)

This document is provided without Prejudice to support Third Country 145 Organisations who believe they may qualify for a Derogation in respect of Information Security – Cyber regulatory obligations.

Introduction - As a Foreign EASA Part 145 organisation, you may apply for a derogation from IS & Cyber requirements (as outlined in Part-IS) under specific conditions.

These conditions are defined in IS.I.OR.200(e) of Regulation (EU) 2023/203 and further elaborated in the Part-IS Implementation Guidelines. The core grounds are:

- No Information Security Risk with Potential Impact on Aviation Safety
  Your organisation must demonstrate that its activities, facilities, and resources, as well as the services it operates, provides, receives, and maintains, do not pose any information security risks that could impact aviation safety—neither to your organisation nor to others.

Note - This involves a comprehensive Information Security Risk Assessment (ISRA), demonstrating that:

- The nature of your maintenance work (e.g., limited to non-safety-critical component maintenance or specific low-risk activities like cleaning, painting, etc.) has no impact on the operational safety of aircraft.
- Your IT systems and data flows are isolated, limited in complexity, and not part of integrated aviation safety systems.
- There are no critical interfaces with other organisations or aviation safety-critical services.

Low Safety Impact and Non-Critical Role in the Aviation Functional Chain
If your organisation:

- Operates in a low-complexity, low-safety-critical domain (e.g., maintenance of non-structural components, no work on avionics or flight control systems),
- Has no significant cross-border activities or dependencies,
- Does not contribute to the structural integrity or critical systems of the aircraft (as illustrated in the guidelines for painting or cleaning services),

You can argue that the nature of your work does not justify full Part-IS compliance.

- **Limited IT Infrastructure and Data Handling**
  If your information systems (used for business operations) are simple, do not handle safety-critical data, and your risk assessment confirms the absence of vulnerabilities or interfaces that could propagate cyber risks, this supports the case for a derogation.

- **Existing Risk Mitigations**
  You must still demonstrate basic protective measures (e.g., confidentiality of information as per IS.I.OR.200(a)(13)) and industry-standard good practices in your organisation, but without full ISMS implementation.

- **Documented Risk Assessment**
  Your risk assessment must justify the exclusion of each Part-IS requirement by clearly showing no risk exposure.
  This assessment should be:

- **Based on a structured methodology,**
- **Include a mapping of your services, systems, and interfaces,**
- **Include a list of key personnel involved in the risk assessment,**
- **Supported by an initial Information Security Risk Assessment (ISRA) that aligns with your organisation's scope of work.**

Next Steps: Prepare and submit the Derogation Documentation Package (as per Annex 2 of the EASA guidelines), including:

- List of affected approvals for which derogation is requested.
- Justification for the exclusion.
- Overview of services, interfaces, and system architecture.
- Initial information security risk assessment.
- Methodology for ISRA and evidence of low/no risk exposure.

Engage proactively with EASA (and any National Authorities, if applicable) to discuss and align on the derogation case.

- Maintain the derogation status through continuous compliance monitoring, prompt notification of scope changes, and regular re-assessment.

4o

Information Security Risk Assessment (ISRA) to Support Derogation Request under IS.I.OR.200(e)

Organisation Information

- Organisation Name: [Your Company Name]
- EASA Part 145 Approval Number: [Insert approval number]
- Primary Scope of Work: [e.g., Maintenance of non-structural components, painting, cleaning, interior refurbishment – *No involvement in structural, avionics, or flight-critical systems*]
- Facilities Location: [Country, Address]
- Key Contact Person: [Name, Position, Email, Phone]

Overview of Activities, Facilities, and Resources

a) Core Business Activities

Our organisation provides component-level maintenance services limited to:

- Non-structural interior components (e.g., cabin fittings, seats, panels)
- Cosmetic services (e.g., aircraft washing, painting, decal application)
- Non-flight-critical parts (e.g., galley units, trolleys, lavatory modules)
- *No engagement in line maintenance, base maintenance, avionics, engines, or structural work.*

b) Facilities and Resources

- Workshop Locations: Standalone facilities with no direct network connections to operational aviation systems.
- IT Systems:
    - Local standalone systems (non-networked) for documentation, billing, and inventory management.

    - No integration with airworthiness data systems, flight planning, or operational control systems.
- Data Handling:
    - Only non-safety-critical data processed (e.g., customer orders, component serial numbers).
    - No handling of operational flight data, avionics software, or aircraft configuration files.

c) External Interfaces

- No direct interfaces with operators' operational systems.
- No data exchange with third-party systems affecting safety-critical functions.
- Occasional email communication for non-critical business coordination.

Risk Identification & Assessment

a) Potential Sources of Information Security Risks

Category	Analysis
IT Infrastructure	Isolated, non-networked local systems; no exposure to aviation safety-critical networks.
Data Processed	No safety-critical data (e.g., no flight control data, avionics software, load sheets, maintenance control documents).
Interfaces	No real-time data exchange or interfaces with other aviation safety organisations.
Third-Party Exposure	No outsourced IT services; no cloud storage of safety-related data.
Services Provided	No activities that impact flight safety, such as airworthiness-critical maintenance or certification.

b) Identified Threats and Likelihood

Threat Scenario	Likelihood	Impact on Aviation Safety	Justification
Malware infection of internal system	Low	None	Systems are standalone, not connected to safety-critical networks.
Accidental data loss	Low	None	Only non-safety data; no impact on flight operations or safety.
Phishing attack	Medium	None	Even if successful, no access to safety-critical systems.
Data manipulation	Low	None	No operational safety data stored.
Supply chain compromise	Low	None	No external IT suppliers involved in critical functions.

c) Residual Risk Conclusion

After evaluation of all potential scenarios, no identified risks pose an impact on aviation safety. Risks are limited to general business continuity (e.g., loss of invoices) and are mitigated through routine backups and basic IT hygiene.

Methodology Used

- Risk Assessment Framework: Aligned with ISO 31000 principles.
- Risk Identification: Mapping of services, facilities, and IT systems against potential impact on aviation safety.
- Risk Analysis: Consideration of likelihood, impact, and exposure within the aviation safety context.
- Risk Evaluation Criteria: Based on the potential impact on the continuing airworthiness, flight safety, or operational integrity of aircraft.
- Risk Treatment: No safety risks identified → Justification for derogation application under IS.I.OR.200(e).

Personnel Involved in the Risk Assessment

Name	Role	Responsibility
[Name]	Accountable Manager	Oversight and final approval of risk assessment.
[Name]	IT/Facilities Manager	Identification and evaluation of IT infrastructure and data flows.
[Name]	Quality/Compliance Manager	Coordination of risk assessment, compliance review.
[Name]	Workshop Supervisor	Validation of operational processes and systems.
[Name]	External Expert (if applicable)	Independent review of risk assessment (if performed).

Conclusion and Justification for Derogation

Based on the above analysis, [Your Organisation] does not pose any information security risks with a potential impact on aviation safety, either to itself or to other organisations.
Our limited scope of work, the nature of services provided, isolated IT environment, and absence of safety-critical data or system interfaces fully support this conclusion.

We therefore respectfully submit this Information Security Risk Assessment as part of our application for derogation under IS.I.OR.200(e) of Regulation (EU) 2023/203.

Commitment to Continuous Monitoring

- We will maintain this assessment under regular review.
- Any change in scope of work, IT infrastructure, or services provided will be immediately notified to the Competent Authority for re-assessment of derogation validity.

Draft Derogation Justification Letter

[Your Organisation Name]
[Your Address]
[City, Country]
[Date]

SOFEMA
AVIATION SERVICES

To:
European Union Aviation Safety Agency (EASA)
Cybersecurity and Emerging Risks Section
Postfach 10 12 53
50452 Köln
Germany
Email: cybersec@easa.europa.eu

Subject: Application for Derogation under IS.I.OR.200(e) – Part-IS Requirements for [Your Organisation Name], EASA Part 145 Approval [Approval Number]

Dear Sir/Madam,

We hereby submit our formal application for a derogation under IS.I.OR.200(e) of Commission Implementing Regulation (EU) 2023/203, regarding the implementation of an Information Security Management System (ISMS) within our organisation.

Justification for the Derogation Request

[Your Organisation Name] is a Foreign EASA Part 145 Approved Maintenance Organisation (Approval Number: [Approval Number]), providing limited-scope services strictly confined to:

- Component-level maintenance of non-safety-critical parts (e.g., cabin interiors, seats, galley units, trolleys).
- Cosmetic and cleaning services (e.g., aircraft washing, paint touch-up, decal application).
- No involvement in structural repairs, avionics, engines, or flight safety-critical systems.

Following a detailed Information Security Risk Assessment (ISRA), conducted in accordance with IS.I.OR.205 and following the methodology recommended by EASA's AMC1 IS.I.OR.200(e) and related guidelines, we confirm that:

- Our activities, facilities, resources, and the services we operate, provide, receive, and maintain do not pose any information security risks that could have a potential impact on aviation safety—either to ourselves or to other organisations.
- Our IT systems are isolated, standalone, and non-integrated with any external aviation safety-critical systems.

- The data processed is limited to general administrative records (e.g., invoicing, inventory) and does not include any flight-critical, operational, or airworthiness-related information.
- We have no interfaces or dependencies on external systems or third-party networks handling safety-critical aviation data.
- We remain committed to protecting the confidentiality of any sensitive information we may receive, as per IS.I.OR.200(a)(13).

In view of the above, we respectfully request the approval of a derogation from the implementation of the requirements outlined in IS.I.OR.200(a) to (d) and IS.I.OR.205 through IS.I.OR.260.

We have enclosed our Information Security Risk Assessment and Documentation Package as required.

We remain at your disposal for any clarification or further information you may require and look forward to your favourable consideration of our application.

Yours sincerely,
[Name]
[Position]
[Your Organisation Name]
[Email]
[Phone]

Derogation Documentation Package – Part-IS Annex 2

Affected Approvals for Derogation

- EASA Part 145 Approval Number: [Insert Approval Number]

Justification for Exclusion of Provisions

- Scope of activities strictly limited to non-safety-critical component maintenance and cosmetic services.
- No engagement in flight safety-critical systems, avionics, engines, or structural repairs.
- IT systems are isolated, with no integration into aviation operational networks.
- No processing of safety-critical data.

- No interfaces with external safety systems or third-party service providers handling safety-related information.

Overview of Services Provided and Received

- Provided Services: Non-structural maintenance, painting, cleaning, minor component handling.
- Received Services: General logistics, material supply (non-safety-critical), office IT support (local only).
- No services provided or received involve safety-critical data or systems.

Architecture of Information Systems

- Local servers with no external network connections.
- Isolated desktops for administrative tasks only.
- No SCADA, PLC, or integrated systems linked to aircraft safety systems.
- No access to operator or regulatory safety data repositories.

Methodology for Information Security Risk Assessment

- Aligned with ISO 31000 and EASA AMC1 IS.I.OR.205(a).
- Systematic mapping of services, systems, interfaces.
- Threat identification based on asset analysis, external dependencies, and potential vulnerabilities.
- Evaluation of risks based on likelihood, severity, and safety impact criteria.
- Conclusion: No information security risks with potential impact on aviation safety identified.

Initial Information Security Risk Assessment

(Included as separate document; summarised in the letter above)

Personnel Involved in Risk Assessment

Name	Role	Responsibility
[Name]	Accountable Manager	Final authority, oversight

Name	Role	Responsibility
[Name]	Compliance Manager	Risk assessment lead
[Name]	IT/Facilities Manager	System architecture and data flows
[Name]	Workshop Supervisor	Process mapping and risk identification

8. Third Parties Involved

- None. All ISRA activities conducted internally, no outsourced risk assessment services utilised.

Final Steps

- Finalise the letter and documentation with your organisation's letterhead, signatures, and company details.
- Submit to EASA via the appropriate contact channels (cybersec@easa.europa.eu) with a copy to your assigned Team Leader, as per your existing oversight relationship.
- Retain a copy of the full package for your internal records.

Sofema Aviation Services and Sofema Online provide EASA Regulatory compliant training as Classroom, Webinar & Online Training including information & Cyber Security – Please see the websites or email team@sassofia.com