European Union Aviation Safety Agency

Derogation

My organisation would like to apply for a derogation. Is it eligible and if so, what procedure should be followed?

Answer

As per GM1 IS.D.OR.200(e):

‘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 by performing a documented information security risk assessment following the procedure outlined in AMC1 IS.D.OR.200(e).’

Indicatively, such organisations might include design organisation approval (DOA) or production organisation approval (POA) holders that design or produce only components or parts that either are not involved in ensuring the structural integrity of the aircraft (e.g., carpets, interiors) or have no major safety-related aircraft functionalities, including but not limited to, aircraft software, navigation, avionics, engines, flight control, landing gear, hydraulic, electrical, air, communications, etc..

The aforementioned example is only indicative of what could 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 information security management system (ISMS). It is up to the authority to determine whether the assessment provided by the organisation is deemed satisfactory for a derogation to be granted. More information on the derogation process.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/fi/faq/139294

If my organisation receives a derogation, does this mean that it is exempted from compliance with Part-IS?

Answer

A derogation is a temporary exemption from the full requirements of the Regulation. The organisation is advised to remain vigilant and, as a minimum, reassess its exposure to cybersecurity threats whenever the scope changes. In particular, 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.

There are a few requirements that still apply or partially apply to a derogated organisation. More information on this and the derogation process.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/fi/faq/139295

Is the derogation provision under point IS.D.OR.200(e) or point IS.I.OR.200(e) linked to the flexibility provisions of Article 71 of the Basic Regulation?

Answer

Point IS.D.OR.200(e) of the Annex (Part-IS.D.OR) to Commission Delegated Regulation (EU) 2022/1645 or IS.I.OR.200(e) of Annex II (Part-IS.I.OR) to Commission Implementing Regulation (EU) 2023/203 provide for a self-contained derogation possibility which can be used independently of Article 71. Those points allow an organisation to be temporarily exempted from implementing an information security management system, provided that its activities, facilities, resources, and services do not pose any information security risks that could affect aviation safety. Therefore, the two are not linked.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/fi/faq/142361