European Union Aviation Safety Agency

Supply chain

Does Part-IS have requirements on suppliers/subcontractors that although they are not within the list of the organisations that have to comply with Part-IS, they work with/for an organisation that is within the Part-IS scope?

Answer

Part-IS requirements are addressed to organisations within the scope of the rules (Article 2 'Scope' of Commission Implementing Regulation (EU) 2023/203 and Commission Delegated Regulation (EU) 2022/1645). These organisations need to address the information security risks at the interfaces with other organisations, whether the latter are within or outside the scope of the rule. To do so, organisations within the scope have two options:

1. they can either implement mitigation measures and controls within their own organisational boundaries; or
2. they may decide instead to manage the risks through contractual agreements and require the supplier/subcontractor to implement mitigation measures and controls within its own organisation.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/en/faq/142368

Is IS.I.OR.235 applicable to all suppliers/subcontractors?

Answer

No. The requirement of point IS.I.OR.235 of Annex II (Part-IS.I.OR) to Commission Implementing Regulation (EU) 2023/203 is applicable only to those suppliers/subcontractors that perform tasks pertinent to information security management activities. All the rest are covered by point IS.I.OR.205 to Part-IS.I.OR.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/en/faq/142369

Can Part-IS implementation and/or the Part-IS compliance monitoring function be subcontracted? If yes, is the subcontracted organisation responsible for implementation and compliance?

Answer

Yes, Part-IS implementation and/or its compliance monitoring function can be subcontracted. It is important to note that the responsibility for performing tasks pertinent to Part-IS can be transferred, accountability however cannot. The organisation subject to Part-IS is always accountable for the implementation of the rule and for demonstration of compliance to the rule. This should be clarified in the agreement between the organisation subject to Part-IS and the subcontractor.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/en/faq/142370

Some or all of our ISMS activities are provided by our corporate IT services. Should these activities be considered as IS.OR.235 activities, given that they are outside the approved/declared organisational structure?

Answer

Yes, and the reason for this is twofold. Firstly, by doing so, the organisation can ensure that the risks associated with these activities are managed appropriately in line with the risk management process. Secondly, the organisation must ensure that the necessary arrangements are in place to enable the CA to oversee the IS service provider.

The risks stemming from the interfaces and the criticality of the provided services should be considered, assessed and documented during the risk management process.

Last updated:
15/06/2026

Link:
https://www.easa.europa.eu/en/faq/143742