Council of the
European Union

Brussels, 18 July 2022
(OR. en)

11468/22
ADD 1

AVIATION 171
DELACT 120

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	14 July 2022
To:	General Secretariat of the Council
No. Cion doc.:	C(2022) 4882 final - ANNEX
Subject:	ANNEX to the COMMISSION DELEGATED REGULATION laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 748/2012 and No 139/2014 and amending Commission Regulations (EU) No 748/2012 and No 139/2014

Delegations will find attached document C(2022) 4882 final - ANNEX.

Encl.: C(2022) 4882 final - ANNEX

EUROPEAN
COMMISSION

Brussels, 14.7.2022
C(2022) 4882 final

ANNEX

ANNEX

to the

COMMISSION DELEGATED REGULATION

laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 748/2012 and No 139/2014 and amending Commission Regulations (EU) No 748/2012 and No 139/2014

ANNEX

INFORMATION SECURITY — ORGANISATION REQUIREMENTS

[PART-IS.D.OR]

IS.D.OR.100 Scope

This Part establishes the requirements to be met by the organisations referred to in Article 2 of this Regulation.

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

(a) In order to achieve the objectives set out in Article 1, the organisation shall set up, implement and maintain an information security management system (ISMS) which ensures that the organisation:

(1) establishes a policy on information security setting out the overall principles of the organisation with regard to the potential impact of information security risks on aviation safety;

(2) identifies and reviews information security risks in accordance with point IS.D.OR.205;

(3) defines and implements information security risk treatment measures in accordance with point IS.D.OR.210;

(4) implements an information security internal reporting scheme in accordance with point IS.D.OR.215;

(5) defines and implements, in accordance with point IS.D.OR.220, the measures required to detect information security events, identifies those events which are considered incidents with a potential impact on aviation safety except as permitted by point IS.D.OR.205(e), and responds to, and recovers from, those information security incidents;

(6) implements the measures that have been notified by the competent authority as an immediate reaction to an information security incident or vulnerability with an impact on aviation safety;

(7) takes appropriate action, in accordance with point IS.D.OR.225, to address findings notified by the competent authority;

(8) implements an external reporting scheme in accordance with point IS.D.OR.230 in order to enable the competent authority to take appropriate actions;

(9) complies with the requirements contained in point IS.D.OR.235 when contracting any part of the activities referred to in point IS.D.OR.200 to other organisations;

(10) complies with the personnel requirements laid down in point IS.D.OR.240;

(11) complies with the record-keeping requirements laid down in point IS.D.OR.245;

(12) monitors compliance of the organisation with the requirements of this Regulation and provides feedback on findings to the accountable manager or, in the case of design organisations, to the head of the design organisation, in order to ensure effective implementation of corrective actions;

(13) protects, without prejudice to applicable incident reporting requirements, the confidentiality of any information that the organisation may have received from other organisations, according to its level of sensitivity.

(b) In order to continuously meet the requirements referred to in Article 1, the organisation shall implement a continuous improvement process in accordance with point IS.D.OR.260.

(c) The organisation shall document, in accordance with point IS.D.OR.250, all key processes, procedures, roles and responsibilities required to comply with point IS.D.OR.200(a) and establish a process for amending that documentation. Changes to those processes, procedures, roles and responsibilities shall be managed in accordance with point IS.D.OR.255.

(d) The processes, procedures, roles and responsibilities established by the organisation in order to comply with point IS.D.OR.200(a) shall correspond to the nature and

complexity of its activities, based on an assessment of the information security risks inherent to those activities, and may be integrated within other existing management systems already implemented by the organisation.

(e) Without prejudice to the obligation to comply with the reporting requirements contained in Regulation (EU) No 376/2014([1]) and the requirements of point IS.D.OR.200 (a) (13), the organisation may be granted approval by the competent authority not to implement the requirements referred to in points (a) to (d)) and the related requirements contained in points IS.D.OR.205 through IS.D.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.D.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.

IS.D.OR.205 Information security risk assessment

(a) The organisation shall identify all of its elements, which could be exposed to information security risks. That shall include:

(1) the organisation's activities, facilities and resources, as well as the services the organisation operates, provides, receives or maintains;

(2) the equipment, systems, data and information that contribute to the functioning of the elements listed in point (1).

(b) The organisation shall identify the interfaces that it has with other organisations, and which could result in the mutual exposure to information security risks.

(c) With regard to the elements and interfaces referred to in points (a) and (b), the organisation shall identify the information security risks which may have a potential impact on aviation safety. For each identified risk, the organisation shall:

(1) assign a risk level according to a predefined classification established by the organisation;

(2) associate each risk and its level with the corresponding element or interface identified in accordance with points (a) and (b).

([1]) Regulation (EU) No 376/2014 of the European Parliament and of the Council of 3 April 2014 on the reporting, analysis and follow-up of occurrences in civil aviation, amending Regulation (EU) No 996/2010 of the European Parliament and of the Council and repealing Directive 2003/42/EC of the European Parliament and of the Council and Commission Regulations (EC) No 1321/2007 and (EC) No 1330/2007 (OJ L 122, 24.4.2014, p. 18).

The predefined classification referred to in point (1) shall take into account the potential of occurrence of the threat scenario and the severity of its safety consequences. Based on that classification, and taking into account whether the organisation has a structured and repeatable risk management process for operations, the organisation shall be able to establish whether the risk is acceptable or needs to be treated in accordance with point IS.D.OR.210.

In order to facilitate the mutual comparability of risks assessments, the assignment of the risk level pursuant to point (1) shall take into account relevant information acquired in coordination with the organisations referred to in point (b).

(d) The organisation shall review and update the risk assessment carried out in accordance with points (a), (b) and (c) in any of the following situations:

(1) there is a change in the elements subject to information security risks;

(2) there is a change in the interfaces between the organisation and other organisations, or in the risks communicated by the other organisations;

(3) there is a change in the information or knowledge used for the identification, analysis and classification of risks;

(4) there are lessons learnt from the analysis of information security incidents.

IS.D.OR.210 Information security risk treatment

(a) The organisation shall develop measures to address unacceptable risks identified in accordance with point IS.D.OR.205, implement them in a timely manner and check their continued effectiveness. Those measures shall enable the organisation to:

(1) control the circumstances that contribute to the effective occurrence of the threat scenario;

(2) reduce the consequences on aviation safety associated with the materialisation of the threat scenario;

(3) avoid the risks.

Those measures shall not introduce any new potential unacceptable risks to aviation safety.

(b) The person referred to in point IS.D.OR.240 (a) and (b) and other affected personnel of the organisation shall be informed of the outcome of the risk assessment carried out in accordance with point IS.D.OR.205, the corresponding threat scenarios and the measures to be implemented.

The organisation shall also inform organisations with which it has an interface in accordance with point IS.D.OR.205(b) of any risk shared between both organisations.

IS.D.OR.215 Information security internal reporting scheme

(a) The organisation shall establish an internal reporting scheme to enable the collection and evaluation of information security events, including those to be reported pursuant to point IS.D.OR.230.

(b) That scheme and the process referred to in point IS.D.OR.220 shall enable the organisation to:

(1) identify which of the events reported pursuant to point (a) are considered information security incidents or vulnerabilities with a potential impact on aviation safety;

(2) identify the causes of, and contributing factors to, the information security incidents and vulnerabilities identified in accordance with point (1), and address them as part of the information security risk management process in accordance with points IS.D.OR.205 and IS.D.OR.220;

(3) ensure an evaluation of all known, relevant information relating to the information security incidents and vulnerabilities identified in accordance with point (1);

(4) ensure the implementation of a method to distribute internally the information as necessary.

(c) Any contracted organisation which may expose the organisation to information security risks with a potential impact on aviation safety shall be required to report information security events to the organisation. Those reports shall be submitted using the procedures established in the specific contractual arrangements and shall be evaluated in accordance with point (b).

(d) The organisation shall cooperate on investigations with any other organisation that has a significant contribution to the information security of its own activities.

(e) The organisation may integrate that reporting scheme with other reporting schemes it has already implemented.

IS.D.OR.220 Information security incidents — detection, response and recovery

(a) Based on the outcome of the risk assessment carried out in accordance with point IS.D.OR.205 and the outcome of the risk treatment performed in accordance with point IS.D.OR.210, the organisation shall implement measures to detect incidents and vulnerabilities that indicate the potential materialisation of unacceptable risks and which may have a potential impact on aviation safety. Those detection measures shall enable the organisation to:

(1) identify deviations from predetermined functional performance baselines;

(2) trigger warnings to activate proper response measures, in case of any deviation.

(b) The organisation shall implement measures to respond to any event conditions

identified in accordance with point (a) that may develop or have developed into an information security incident. Those response measures shall enable the organisation to:

(1) initiate the reaction to the warnings referred to in point (a)(2) by activating predefined resources and course of actions;

(2) contain the spread of an attack and avoid the full materialisation of a threat scenario;

(3) control the failure mode of the affected elements defined in point IS.D.OR.205(a).

(c) The organisation shall implement measures aimed at recovering from information security incidents, including emergency measures, if needed. Those recovery measures shall enable the organisation to:

(1) remove the condition that caused the incident, or constrain it to a tolerable level;

(2) reach a safe state of the affected elements defined in point IS.D.OR.205(a) within a recovery time previously defined by the organisation.

IS.D.OR.225 Response to findings notified by the competent authority

(a) After receipt of the notification of findings submitted by the competent authority, the organisation shall:

(1) identify the root cause or causes of, and contributing factors to, the non-compliance;

(2) define a corrective action plan;

(3) demonstrate the correction of the non-compliance to the satisfaction of the competent authority.

(b) The actions referred to in point (a) shall be carried out within the period agreed with the competent authority.

IS.D.OR.230 Information security external reporting scheme

(a) The organisation shall implement an information security reporting system that complies with the requirements laid down in Regulation (EU) No 376/2014 and its delegated and implementing acts if that Regulation is applicable to the organisation.

(b) Without prejudice to the obligations of Regulation (EU) 376/2014, the organisation shall ensure that any information security incident or vulnerability, which may represent a significant risk to aviation safety, is reported to their competent authority. Furthermore:

(1) where such an incident or vulnerability affects an aircraft or associated system or component, the organisation shall also report it to the design approval holder;

(2) where such an incident or vulnerability affects a system or constituent used by the organisation, the organisation shall report it to the organisation responsible for the design of the system or constituent.

(c) The organisation shall report the conditions referred to in point (b) as follows:

(1) a notification shall be submitted to the competent authority and, if applicable, to the design approval holder or to the organisation responsible for the design of the system or constituent, as soon as the condition has been known to the organisation;

(2) a report shall be submitted to the competent authority and, if applicable, to the design approval holder or to the organisation responsible for the design of the system or constituent, as soon as possible, but not exceeding 72 hours from the time the condition has been known to the organisation, unless exceptional circumstances prevent this.

The report shall be made in the form defined by the competent authority and shall contain all relevant information about the condition known to the organisation;

(3) a follow-up report shall be submitted to the competent authority and, if applicable, to the design approval holder or to the organisation responsible for the design of the system or constituent, providing details of the actions the organisation has taken or intends to take to recover from the incident and the actions it intends to take to prevent similar information security incidents in the future.

The follow-up report shall be submitted as soon as those actions have been identified, and shall be produced in the form defined by the competent authority.

IS.D.OR.235 Contracting of information security management activities

(a) The organisation shall ensure that when contracting any part of the activities referred to in point IS.D.OR.200 to other organisations, the contracted activities comply with the requirements of this Regulation and the contracted organisation works under its oversight. The organisation shall ensure that the risks associated with the contracted activities are appropriately managed.

(b) The organisation shall ensure that the competent authority can have access upon request to the contracted organisation to determine continued compliance with the applicable requirements laid down in this Regulation.

IS.D.OR.240 Personnel requirements

(a) The accountable manager of the organisation or, in the case of design organisations, the head of the design organisation, designated in accordance with Regulation (EU) No 748/2012 and Regulation (EU) No 139/2014 as referred to in points 1(a) and (b) of Article 2 of this Regulation, shall have corporate authority to ensure that all activities required by this Regulation can be financed and carried out. That person shall:

(1) ensure that all necessary resources are available to comply with the requirements

of this Regulation;

(2) establish and promote the information security policy referred to in point IS.D.OR.200(a)(1);

(3) demonstrate a basic understanding of this Regulation.

(b) The accountable manager or, in the case of design organisations, the head of the design organisation, shall appoint a person or group of persons to ensure that the organisation is in compliance with the requirements of this Regulation, and shall define the extent of their authority. That person or group of persons shall report directly to the accountable manager or, in the case of design organisations, to the head of the design organisation, and shall have the appropriate knowledge, background and experience to discharge their responsibilities. It shall be determined in the procedures who deputises for a particular person in the case of lengthy absence of that person.

(c) The accountable manager or, in the case of design organisations, the head of the design organisation shall appoint a person or group of persons with the responsibility to manage the compliance monitoring function referred to in point IS.D.OR.200(a)(12).

(d) Where the organisation shares information security organisational structures, policies, processes and procedures, with other organisations or with areas of their own organisation which are not part of the approval or declaration, the accountable manager or, in the case of design organisations, the head of the design organisation, may delegate its activities to a common responsible person.

In such a case, coordination measures shall be established between the accountable manager of the organisation or, in the case of design organisations, the head of the design organisation, and the common responsible person to ensure adequate integration of the information security management within the organisation.

(e) The accountable manager or the head of the design organisation, or the common responsible person referred to in point (d), shall have corporate authority to establish and maintain the organisational structures, policies, processes and procedures necessary to implement point IS.D.OR.200.

(f) The organisation shall have a process in place to ensure that they have sufficient personnel on duty to carry out the activities covered by this Annex.

(g) The organisation shall have a process in place to ensure that the personnel referred to in point (f) have the necessary competence to perform their tasks.

(h) The organisation shall have a process in place to ensure that personnel acknowledge the responsibilities associated with the assigned roles and tasks.

(i) The organisation shall ensure that the identity and trustworthiness of the personnel who have access to information systems and data subject to the requirements of this Regulation are appropriately established.

IS.D.OR.245 Record-keeping

(a) The organisation shall keep records of its information security management activities

(1) The organisation shall ensure that the following records are archived and traceable:

(i) any approval received and any associated information security risk assessment in accordance with point IS.D.OR.200(e);

(ii) contracts for activities referred to in point IS.D.OR.200(a)(9);

(iii) records of the key processes referred to in point IS.D.OR.200(d);

(iv) records of the risks identified in the risk assessment referred to in point IS.D.OR.205 along with the associated risk treatment measures referred to in point IS.D.OR.210;

(v) records of information security incidents and vulnerabilities reported in accordance with the reporting schemes referred to in points IS.D.OR.215 and IS.D.OR.230;

(vi) records of those information security events which may need to be reassessed to reveal undetected information security incidents or vulnerabilities.

(2) The records referred to in point (1)(i) shall be retained at least until 5 years after the approval has lost its validity.

(3) The records referred to in point (1)(ii) shall be retained at least until 5 years after the contract has been amended or terminated.

(4) The records referred to in point (1)(iii), (iv) and (v) shall be retained at least for a period of 5 years.

(5) The records referred to in point (1)(vi) shall be retained until those information security events have been reassessed in accordance with a periodicity defined in a procedure established by the organisation.

(b) The organisation shall keep records of qualification and experience of its own staff involved in information security management activities

(1) The personnel's qualification and experience records be retained for as long as the person works for the organisation, and for at least 3 years after the person has left the organisation.

(2) Members of the staff shall, upon their request, be given access to their individual records. In addition, upon their request, the organisation shall provide them with a copy of their individual records on leaving the organisation.

(c) The format of the records shall be specified in the organisation's procedures.

(d) Records shall be stored in a manner that ensures protection from damage, alteration and theft, with information being identified, when required, according to its security classification level. The organisation shall ensure that the records are stored using means to ensure integrity, authenticity and authorised access.

IS.D.OR.250 Information security management manual (ISMM)

(a) The organisation shall make available to the competent authority an information security management manual (ISMM) and, where applicable, any referenced associated manuals and procedures, containing:

(1) a statement signed by the accountable manager or, in the case of design organisations, by the head of the design organisation, confirming that the organisation will at all times work in accordance with this Annex and with the ISMM. If the accountable manager or, in the case of design organisations, the head of the design organisation, is not the chief executive officer (CEO) of the organisation, then such CEO shall countersign the statement;

(2) the title(s), name(s), duties, accountabilities, responsibilities and authorities of the person or persons referred to in point IS.D.OR.240(b) and (c);

(3) the title, name, duties, accountabilities, responsibilities and authorities of the common responsible person referred to in point IS.D.OR.240(d), if applicable;

(4) the information security policy of the organisation as referred to in point IS.D.OR.200(a)(1);

(5) a general description of the number and categories of staff and of the system in place to plan the availability of staff as required by point IS.D.OR.240;

(6) the title(s), name(s), duties, accountabilities, responsibilities and authorities of the key persons responsible for the implementation of point IS.D.OR.200, including the person or persons responsible for the compliance monitoring function referred to in point IS.D.OR.200(a)(12);

(7) an organisation chart showing the associated chains of accountability and responsibility for the persons referred to in points (2) and (6);

(8) the description of the internal reporting scheme referred to in point IS.D.OR.215;

(9) the procedures that specify how the organisation ensures compliance with this Part, and in particular:

(i) the documentation point IS.D.OR.200(c);

(ii) the procedures that define how the organisation controls any contracted activities referred to in point IS.D.OR.200(a)(9);

(iii) the ISMM amendment procedure defined in point (c);

(10) the details of currently approved alternative means of compliance.

(b) The initial issue of the ISMM shall be approved and a copy shall be retained by the competent authority. The ISMM shall be amended as necessary to remain an up-to-date description of the ISMS of the organisation. A copy of any amendments to the ISMM shall be provided to the competent authority.

(c) Amendments to the ISMM shall be managed in a procedure established by the organisation. Any amendments that are not included within the scope of this procedure

and any amendments related to the changes referred to in point IS.D.OR.255(b), shall be approved by the competent authority.

(d) The organisation may integrate the ISMM with other management expositions or manuals it holds, provided there is a clear cross reference that indicates which portions of the management exposition or manual correspond to the different requirements contained in this Annex.

IS.D.OR.255 Changes to the information security management system

(a) Changes to the ISMS may be managed and notified to the competent authority in a procedure developed by the organisation. This procedure shall be approved by the competent authority.

(b) With regard to changes to the ISMS not covered by the procedure referred to in point (a), the organisation shall apply for and obtain an approval issued by the competent authority.

With regard to these changes:

(1) the application shall be submitted before any such change takes place, in order to enable the competent authority to determine continued compliance with this Regulation and to amend, if necessary, the organisation certificate and related terms of approval attached to it;

(2) the organisation shall make available to the competent authority any information it requests to evaluate the change;

(3) the change shall be implemented only upon receipt of a formal approval by the competent authority;

(4) the organisation shall operate under the conditions prescribed by the competent authority during the implementation of such changes.

IS.D.OR.260 Continuous improvement

(a) The organisation shall assess, using adequate performance indicators, the effectiveness and maturity of the ISMS. That assessment shall be carried out on a calendar basis predefined by the organisation or following an information security incident.

(b) If deficiencies are found following the assessment carried out in accordance with point (a), the organisation shall take the necessary improvement measures to ensure that the ISMS continues to comply with the applicable requirements and maintains the information security risks at an acceptable level. In addition, the organisation shall reassess those elements of the ISMS affected by the adopted measures.