EUROPEAN
COMMISSION

Brussels, XXX
[…](2021) XXX draft

**ANNEX IV TO EASA OPINION 03 -2021**

**COMMISSION DELEGATED REGULATION (EU) …/...**

**of XXX**

**introducing 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**

# EXPLANATORY MEMORANDUM

## 1. CONTEXT OF THE DELEGATED ACT

The current European aviation safety regulatory framework contains a series of requirements which are aimed at reducing the likelihood of an accident happening.

This combination of requirements allows that even if an error, mistake and/or deficiency happens, it should not create a hazardous situation that could result in an accident or serious incident. Consequently, an accident or serious incident would only happen in the remote random event of several deficiencies happening simultaneously and, by chance, aligning themselves.

The concern is that not enough focus may have been put in properly addressing the situation where existing flaws in different areas are aligned on purpose and exploited by individuals with a malicious intent, no longer being a random event. Such a risk is constantly increasing in the civil aviation environment as the current information systems are becoming more and more interconnected.

As a consequence, it is necessary to introduce requirements for the management of information security risks which could have a potential impact on aviation safety.

In the particular case of this Delegated Act, the provisions introduced increase the robustness of the management systems and reporting processes and procedures required by Annex II 'Essential requirements for airworthiness' and Annex VII 'Essential requirements for aerodromes' to Regulation (EU) 2018/1139 ([1]) for design and production organisations, and for aerodrome operators and providers of apron management services.

## 2. CONSULTATIONS PRIOR TO THE ADOPTION OF THE ACT

In accordance with Article 128(4) of Regulation (EU) 2018/1139, before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making. The present draft delegated act was presented to the Air Safety experts group, which includes representatives from the Member States, at its meeting on […]. The present draft delegated act is based on EASA Opinion No 03/2021 whose contents had been publicly consulted through Notice of Proposed Amendment (NPA) 2019-07 'Management of information security risks' ([2]) (RMT.0720), published by EASA on 27 May 2019.

---

([1]) Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1) (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1535612134845&uri=CELEX:32018R1139).

([2]) https://www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2019-07

## 3. LEGAL ELEMENTS OF THE DELEGATED ACT

Articles 19(1) and 39(1) of Regulation (EU) 2018/1139 empower the Commission to adopt delegated acts, in accordance with Article 128 of that Regulation, laying down detailed rules with regard to organisations responsible for the design and production of products, parts and non-installed equipment, and with regard to organisations responsible for the operation of aerodromes and for the provision of apron management services.

**COMMISSION DELEGATED REGULATION (EU) …/...**

**of XXX**

**introducing 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**

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 ([3]), and in particular Articles 19(1) and 39(1) thereof,

Whereas:

(1) In accordance with the essential requirements set out in Annex II to Regulation (EU) 2018/1139, design and production organisations shall implement and maintain a management system to manage safety risks.

(2) In addition, in accordance with the essential requirements set out in Annex VII to Regulation (EU) 2018/1139, aerodrome operators and organisations responsible for the provision of apron management services shall implement and maintain a management system to manage safety risks.

(3) The management systems implemented by those organisations to manage safety risks need to take into account not only those risks stemming for random events, but also those where existing flaws may be exploited by individuals with a malicious intent.

(4) This type of risks is constantly increasing in the civil aviation environment as the current information systems are becoming more and more interconnected, and increasingly becoming the target of malicious actors.

(5) The risks associated with these information systems are not limited to possible attacks to the cyberspace, but encompass threats which are both digital and analogue.

(6) A significant number of organisations already use international standards, such as ISO 27001, which deal with the management of information security risks.

(7) As a consequence, it is appropriate to introduce requirements for the management of information security risks, without limiting them to cybersecurity risks.

(8) It is essential that these requirements cover the different aviation domains and their interfaces since aviation is a highly interconnected system of systems. As a consequence, they shall apply to all the organisations and competent authorities that are already required to have a management system in accordance with the existing aviation safety regulations.

([3]) OJ L 212, 22.8.2018, p. 1.

(9) The measures provided for in this Regulation need to contribute to the creation of a seamless and consistent regulatory framework where the interfaces between security and safety are appropriately covered, and where special attention is paid at avoiding gaps, loopholes and duplications with other information security and cybersecurity requirements such as those contained in Commission Implementing Regulation (EU) 2015/1998 ([4]) and in the national requirements stemming from Directive (EU) 2016/1148 (NIS Directive) ([5]).

(10) The measures related to information security and cybersecurity stemming from the NIS Directive, Commission Implementing Regulation (EU) 2015/1998 and this Regulation should be coordinated at national levels to avoid gaps and duplications of obligations.

(11) It is therefore appropriate that, where organisations covered by this Regulation are subject to cybersecurity or information security requirements arising from other EU or national legislation, the competent authority defined according to this Regulation should have the possibility to replace compliance with the requirements of this Regulation by compliance with elements contained in other EU or national legislation, provided that such requirements are at least equivalent in effect to the obligations laid down in this Regulation. In such a case, the competent authority shall coordinate with any other relevant authorities to ensure coordinated or compatible oversight regimes.

(12) In addition, in the particular case of airport operators, air carriers and entities as defined in the national civil aviation security programmes of Member States, it is appropriate that the competent authority responsible for the certification and oversight of the organisation's compliance with this Regulation should have the possibility to replace compliance with the requirements contained in this Regulation, except those related to the information security external reporting schemes, by compliance with elements of the cybersecurity requirements contained in the Annex to Implementing Regulation (EU) 2015/1998. In such a case, the competent authority shall coordinate with any other relevant authorities to ensure coordinated or compatible oversight regimes.

(13) Furthermore, it is also appropriate that even if the competent authority decides not to use the options described in the previous two recitals, the affected organisations should still have the possibility to use compliance methods developed under the cybersecurity or information security requirements of those EU or national legislations as a means to comply with the requirements of this Regulation, In such a case, the organisation shall demonstrate to their competent authority that with those compliance methods the organisation fully meets the requirements and objectives of this Regulation.

(14) The measures provided for in this Regulation need to ensure a consistent implementation across all aviation domains, while creating a minimal impact on the existing rules already applicable to those domains.

(15) The measures provided for in this Regulation need to be proportional to the risks incurred by the different organisations.

(16) The measures provided for in this Regulation need to follow a performance- and risk-based approach.

---

([4]) Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security (OJ L 299, 14.11.2015, p. 1).

([5]) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

(17) The measures provided for in this Regulation need to ensure that organisations can integrate any new management system requirements with other existing management systems they may have.

(18) A sufficient transition period should be provided for organisations to ensure their compliance with the new rules and procedures introduced by this Regulation.

(19) The measures provided for in this Regulation are based on Opinion No 03/2021 ([6]), issued by the European Union Aviation Safety Agency in accordance with Article 75(2)(b) and (c) and Article 76(1) of Regulation (EU) 2018/1139.

(20) The measures provided for in this Regulation are in accordance with the opinion of the committee established by Article 127 of Regulation (EU) 2018/1139,

HAS ADOPTED THIS REGULATION:

*Article 1*

**Objectives**

This Regulation establishes the requirements to be met by the organisations and competent authorities referred to in Article 2 in order to:

— identify and manage information security risks which could affect information and communication technology systems and data used for civil aviation purposes,

— detect information security events identifying those which are considered information security incidents, and

— respond to, and recover from, those information security incidents,

to a level commensurate with their impact on aviation safety.

*Article 2*

**Scope**

1. This Regulation applies to:

(a) production organisations and design organisations subject to Subparts G and J respectively of Section A of Annex I (Part 21) to Regulation (EU) No 748/2012 ([7]), except those design organisations solely involved in the design of ELA2 aircraft;

([6]) https://www.easa.europa.eu/document-library/opinions

([7]) Commission Regulation (EU) No 748/2012 of 3 August 2012 laying down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and production organisations (OJ L 224, 21.8.2012, p. 1).

(b) aerodrome operators and apron management service providers subject to Annex III 'Part Organisation Requirements (Part-ADR.OR)' to Regulation (EU) No 139/2014 ([8]).

This Regulation is referenced in the regulations listed in points (1)(a) and (1)(b) of this Article, and compliance with its requirements shall be an integral part of the organisation approval or declaration required by those regulations.

2. Organisations within the scope of Article 2(1) shall comply with the requirements of Annex I (Part-IS.OR) to this Regulation.

*Article 3*

**Organisations subject to cybersecurity or information security requirements arising from other EU or national legislation**

1. Without prejudice to paragraph 2, where organisations listed in points (1)(a) and (1)(b) of Article 2 of this Regulation are subject to cybersecurity or information security requirements arising from other EU or national legislation, the competent authority responsible for the certification and oversight of the organisation's compliance with this Regulation may replace compliance with the requirements of this Regulation by compliance with elements contained in other EU or national legislation, provided that such requirements are at least equivalent in effect to the obligations laid down in this Regulation. In such a case, this competent authority shall coordinate with any other relevant authorities to ensure coordinated or compatible oversight regimes.

2. In the case of airport operators, air carriers and entities as defined in the national civil aviation security programmes of Member States, the competent authority responsible for the certification and oversight of the organisation's compliance with this Regulation may replace compliance with the requirements contained in this Regulation, except those related to the information security external reporting scheme required by point IS.OR.230 of Annex I to this Regulation, by compliance with elements of the cybersecurity requirements contained in the Annex to Commission Implementing Regulation (EU) 2015/1998. In such a case, this competent authority shall coordinate with any other relevant authorities to ensure coordinated or compatible oversight regimes.

3. For those requirements contained in this Regulation where the competent authority has not used the provisions of paragraph 1 or 2, the organisation may use compliance methods developed under the cybersecurity or information security requirements of those EU or national legislation as a means to comply with the requirements of this Regulation, provided that the organisation demonstrates to their competent authority that with those compliance methods the organisation fully meets the requirements and objectives of this Regulation.

*Article 4*

**Definitions**

For the purpose of this Regulation, the following definitions shall apply:

([8]) Commission Regulation (EU) No 139/2014 of 12 February 2014 laying down requirements and administrative procedures related to aerodromes pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council (OJ L 44, 14.2.2014, p. 1).

(a) ‘ELA2 aircraft’ means a manned European Light Aircraft as defined in Article 1(2)(j) of Regulation (EU) No 748/2012;

(b) ‘information security’ means the preservation of confidentiality, integrity and availability of information;

(c) ‘information security event’ means an identified occurrence of a system, service or network state indicating a possible breach of the information security policy or failure of information security controls, or a previously unknown situation that can be relevant for information security;

(d) ‘information security incident’ means a single or a series of unwanted or unexpected events having an actual adverse effect on information security;

(e) ‘information security risk’ means the risk to organisational civil aviation operations, assets, individuals, and other organisations due to the potential of an information security event. Information security risks are associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets;

(f) ‘threat’ means a potential violation of information security which exists when there is an entity, circumstance, action or event that could cause harm;

(g) ‘vulnerability’ means a flaw or weakness in systems, procedures, design, implementation, or information security measures that could be exploited and results in a breach or violation of the information security policy.

*Article 5*

**Competent authority**

In those cases where the competent authority is not the Agency, Member States may designate as the competent authority responsible for the certification and oversight of each organisation’s compliance with this Regulation the same competent authority designated in each one of the Regulations listed in points (1)(a) and (1)(b) of Article 2 of this Regulation. Member States may also designate as competent authority for the purposes of this Regulation a stand-alone entity, independent and autonomous from other competent authorities, in which case coordination measures shall be established between the different entities, in order to ensure effective oversight of all the requirements to be met by the organisation.

*Article 6*

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from [*OP please insert date: **1 year** after the date of entry into force*].

Organisations within the scope of Article 2 may correct any findings of non-compliance related to this Regulation until ***[****OP please insert date: **2 years** after the date of entry into force****]*** or until the date established by the competent authority for the correction of the finding, whichever comes later.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

*For the Commission*
*The President*
*Ursula VON DER LEYEN*

*ANNEX I*

**INFORMATION SECURITY — ORGANISATION REQUIREMENTS**

**[PART-IS.OR]**



**IS.OR.100 Scope**

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

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

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

(1) establishes a policy on information security describing 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.OR.205;

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

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

(5) defines and implements, in accordance with point IS.OR.220, the measures required to detect information security events, identifies those which are considered incidents with a potential impact on aviation safety except as permitted by point IS.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.OR.225, to address findings notified by the competent authority;

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

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

(10) complies with the personnel requirements contained in point IS.OR.240;

(11) complies with the record-keeping requirements contained in point IS.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, 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 objectives described in Article 1, the organisation shall implement a continuous improvement process in accordance with point IS.OR.260.

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

(d) The processes, procedures, roles and responsibilities established by the organisation in order to comply with point IS.OR.200(a) shall correspond to the size of the organisation and the nature and complexity of its activities, taking into account the risks inherent in these 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([9]), the organisation may be approved by the competent authority not to implement the requirements contained in points (a) through (d) if it demonstrates to the satisfaction of such authority that its activities, facilities and resources, as well as the services it operates, provides, receives and maintains, do not pose

([9]) 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).

any information security risks with a potential impact on aviation safety neither to itself nor to other organisations. This approval shall be based on a documented information security risk assessment performed by the organisation in accordance with point IS.OR.205 and reviewed and approved by its competent authority.

The continued validity of this approval shall 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.OR.205 Information security risk assessment**

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

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

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

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

(c) For the elements and interfaces identified 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; and

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

The predefined classification referred to in point (c)(1) shall take into account the potential of occurrence of the threat scenario and the severity of its safety consequences. Through this 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.OR.210.

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

(d) The organisation shall review and update the risk assessment performed under points (a), (b) and (c) when:

(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; or

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

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

**IS.OR.210 Information security risk treatment**

(a) The organisation shall develop measures to address unacceptable risks identified under point IS.OR.205, shall implement them in a timely manner and shall verify their continued effectiveness. Through these measures the organisation shall be able to:

(1) control those circumstances that contribute to the effective occurrence of the threat scenario; and/or

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

(3) avoid the risks.

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

(b) The management and other affected personnel of the organisation shall be informed about the outcome of the risk assessment performed under point IS.OR.205, the corresponding threat scenarios and the measures to be implemented.

The organisation shall also inform those organisations with whom they have an interface in accordance with point IS.OR.205(b) about any shared risk.

**IS.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 under point IS.OR.230.

(b) Through this scheme, and through the process described in point IS.OR.220, the organisation shall:

(1) identify which of the events reported under 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 under point (b)(1), and address them as part of the information security risk management process in accordance with points IS.OR.205 and IS.OR.220;

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

(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. These 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 this reporting scheme with other reporting schemes it has already implemented.

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

(a) Based on the outcome of the risk assessment performed in accordance with point IS.OR.205 and the outcome of the risk treatment performed in accordance with point IS.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. Through these detection measures the organisation shall be able to:

(1) identify deviations from predetermined functional performance baselines; and

(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 under point (a) that may develop or have developed into an information security incident. Through these response measures the organisation shall be able to:

(1) initiate the reaction to the warnings specified under 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; and

(3) control the failure mode of the items in scope.

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

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

(2) reach a safe state of items in scope within a recovery time previously defined by the organisation.

**IS.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; and

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

(b) The actions required by point (a) shall be performed within the period agreed with the competent authority.

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

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

(b) Without prejudice to point (a), 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. In addition:

(1) when 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) when 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 identified 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.

This report shall be made in a form and manner established by the competent authority and shall contain all pertinent 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.

This follow-up report shall be submitted as soon as these actions have been identified, and shall be produced in a form and manner established by the competent authority.

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

(a) The organisation shall ensure that when contracting any part of the activities required by point IS.OR.200 to other organisations, the contracted activities conform to 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 under this Regulation.

**IS.OR.240 Personnel requirements**

(a) The accountable manager of the organisation or, in the case of design organisations, the head of the design organisation, as nominated in accordance with the Regulations detailed in points (1)(a) and (1)(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.

This 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 specified in point IS.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 nominate a person or group of persons to ensure that the organisation is in compliance with the requirements of this Regulation, and shall define the degree of their authority. Such person or group of persons shall be responsible and have direct access 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 made clear 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 nominate a person or group of persons with the responsibility to manage the compliance monitoring function required under point IS.OR.200(a)(12).

(d) In the case 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 described in (d), shall have corporate authority to establish and maintain the organisational structures, policies, processes and procedures necessary to implement point IS.OR.200.

(f) The organisation shall have a process in place to ensure that they have sufficient personnel on duty to perform the activities related to Annex I (Part-IS.OR) to this Regulation.

(g) The organisation shall have a process in place to ensure that the personnel required by (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.OR.245 Record-keeping**

(a) Records of the 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.OR.200(e);

(ii) contracts for activities defined in point IS.OR.200(a)(9);

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

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

(v) records of information security incidents and vulnerabilities reported under the IS.OR.215 and IS.OR.230 internal and external reporting schemes;

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

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

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

(4) The records specified under points (a)(1)(iii), (iv) and (v) shall be retained at least for a period of 5 years.

(5) The records specified under point (a)(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) Personnel records

(1) The organisation shall ensure that the records of qualification and experience of personnel involved in information security management and compliance monitoring are retained.

(2) The records specified under (b)(1) shall 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.

(3) The staff referred to in points (b)(1) and (b)(2) shall, upon their request, be given access to their personnel records as detailed above. In addition, upon their request, the organisation shall furnish them with a copy of their personnel 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.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 Annex I (Part-IS.OR) to this Regulation and with the ISMM. When 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 defined in points IS.OR.240(b) and (c);

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

(4) the information security policy of the organisation as defined in point IS.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.OR.240;

(6) the title(s), name(s), duties, accountabilities, responsibilities and authorities of the key persons responsible for the implementation of point IS.OR.200, including the person or persons responsible for the compliance monitoring function as described in point IS.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 as required by point IS.OR.215;

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

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

(ii) the procedures that define how the organisation controls any contracted activities as required by point IS.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 as defined in a procedure established by the organisation. Any amendments that are not included within the scope of this procedure, as well as any amendments related to the changes listed in point IS.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 Annex I (Part-IS.OR) to this Regulation.

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

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

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

For 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; and

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

**IS.OR.260 Continuous improvement**

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

(b) If deficiencies are found as a result of the assessment performed under point (a), the organisation shall take the necessary improvement measures to ensure that the ISMS stays aligned 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 measures introduced.