European Union Aviation Safety Agency

Explanatory Note to ED Decisions 2023/008/R, 2023/009/R and 2023/010/R

Management of information security risks

Development of acceptable means of compliance and guidance material to support the Part-IS regulatory package implementation

RMT.0720 (SUBTASK 2)

EXECUTIVE SUMMARY

These Decisions issue acceptable means of compliance (AMC) and guidance material (GM) to the Part-IS regulatory package (Regulations (EU) 2022/1645 and 2023/203).

The objective of the AMC and GM is to support and facilitate the application of the new Regulations, thereby maintaining a high level of safety and contributing to the protection of the aviation system against information security (cybersecurity) risks.

REGULATION(S) TO BE AMENDED/ISSUED	**ED DECISIONS TO BE ISSUED**
N/A	ED Decision 2023/008/R — AMC & GM to the Articles of Regulation (EU) 2022/1645 and Regulation (EU) 2023/203 ED Decision 2023/009/R — AMC & GM to Part-IS.D.OR and Part-IS.I.OR ED Decision 2023/010/R — AMC & GM to Part-IS.AR **ED DECISIONS TO BE AMENDED** ED Decision 2012/006/R— AMC & GM to Part-ARA ED Decision 2012/020/R— AMC & GM to Part 21 ED Decision 2014/025/R— AMC & GM to Part-ARO ED Decision 2014/012/R— AMC & GM to Part-ADR.AR ED Decision 2015/029/R— AMC & GM to Part-145 ED Decision 2020/002/R— AMC & GM to Part-CAMO ED Decision 2015/010/R — AMC & GM to Part ATCO.AR ED Decision 2017/001/R— AMC & GM to Part-ATM/ANS.AR

AFFECTED STAKEHOLDERS: DOA and POA holders, air operators, AeMCs, FSTD operators, U-space service providers and single common information service providers, apron management service providers, MOs, CAMOs, training organisations, ATM/ANS providers, aerodrome operators, Member States' national competent authorities (NCAs)

WORKING METHOD(S)

Development	**Impact assessment(s)**	**Consultation**
By EASA with external support	Light	**NPA — Focused** (EASA Advisory Bodies and FAA, TCCA, ANAC Brazil, CAA Israel)

RELATED DOCUMENTS / INFORMATION

ToR RMT.0720, issued on 16.1.2019
Opinion No 03/2021, issued on 11.6.2021
NPA 2023-102, issued on 8.3.2023

PLANNING MILESTONES: Refer to the latest edition of the EPAS Volume II.

Table of contents

1. About these Decisions 3

2. In summary — why and what 5

2.1. Why we need to act — issue/rationale 5
2.2. Assessment of the issue 5
2.3. Who is affected by the issue 5
2.4. What we want to achieve — objectives 5
2.5. What are the stakeholders' views 5

3. What are the expected benefits and drawbacks of the regulatory material 9

4. Monitoring and evaluation 10

5. Proposed actions to support implementation 11

6. References 12

1. About these Decisions

This rulemaking activity aims at developing AMC and GM to the Part-IS regulatory package (Regulations (EU) 2022/1645[1] and 2023/203[2]). It is included in Volume II of the European Plan for Aviation Safety (EPAS) for 2023–2025[3] under Rulemaking Task (RMT).0720 — Subtask 2.

EASA developed the regulatory material in question in line with Regulation (EU) 2018/1139[4] (the Basic Regulation) and the Rulemaking Procedure[5], as well as in accordance with the objectives and working methods described in the Terms of Reference (ToR) for this RMT.

The draft regulatory material was developed with the support of the European Strategic Coordination Platform (ESCP).

The ESCP has been regularly meeting since September 2021 for the development of AMC and GM to the Part-IS regulatory package. Besides EASA, representatives from the following organisations have participated in this activity:

— **ESCP Members**
- European Commission (DG-MOVE);
- other EU agencies and organisations:
  - European Union Agency for Network Information Security (ENISA);
  - EUROCONTROL;
  - European Defence Agency (EDA);

[1] Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 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 (EU) No 139/2014 and amending Commission Regulations (EU) No 748/2012 and (EU) No 139/2014 (OJ L 248, 26.9.2022, p. 18) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1645).

[2] Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 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 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664, and for competent authorities covered by Commission Regulations (EU) No 748/2012, (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340 and (EU) No 139/2014, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664 and amending Commission Regulations (EU) No 1178/2011, (EU) No 748/2012, (EU) No 965/2012, (EU) No 139/2014, (EU) No 1321/2014, (EU) 2015/340, and Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664 (OJ L 31, 2.2.2023, p. 1) (https://eur-lex.europa.eu/eli/reg_impl/2023/203).

[3] European Plan for Aviation Safety 2023-2025 | EASA (europa.eu)

[4] 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).

[5] EASA is bound to follow a structured rulemaking process as required by Article 115(1) of Regulation (EU) 2018/1139. Such a process has been adopted by the EASA Management Board (MB) and is referred to as the 'Rulemaking Procedure'. See MB Decision No 01-2022 of 2 May 2022 on the procedure to be applied by EASA for the issuing of opinions, certification specifications and other detailed specifications, acceptable means of compliance and guidance material ('Rulemaking Procedure'), and repealing Management Board Decision No 18-2015 (https://www.easa.europa.eu/the-agency/management-board/decisions/easa-mb-decision-01-2022-rulemaking-procedure-repealing-mb).

- Six European States' national competent authorities (Finland, France, Italy, Poland, Spain and Switzerland);
- European Civil Aviation Conference (ECAC);
- aviation industry associations:
  - AeroSpace and Defence Industries Association Europe (ASD);
  - Airlines for Europe (A4E);
  - Airports Council International — Europe (ACI);
  - Civil Air Navigation Services Organisation — Europe (CANSO);
  - European Cockpit Association (ECA);
  - European Helicopter Association (EHA);
  - European Regional Airlines Association (ERAA);
  - General Aviation Manufacturers (GAMA);
  - International Air Transport Association — Europe (IATA).

— **ESCP Observers**

- Federal Aviation Administration (FAA), Transport Canada Civil Aviation (TCCA), CAA Israel, Agência Nacional de Aviação Civil (ANAC) Brazil;
- North Atlantic Treaty Organization (NATO);
- Aerospace Industries Association of America (AIA);
- Aviation Information Sharing and Analysis Center (A-ISAC);
- European Business Aviation Association (EBAA).

The draft regulatory material was consulted through focused consultation of NPA 2023-102[6] with the EASA Advisory Bodies (MAB and SAB) as well as with the FAA, the TCCA, the CAA Israel, and ANAC (CAA Brazil).

As part of the focused consultation phase, EASA organised a workshop with the consulted stakeholders on NPA 2023-102 'Development of acceptable means of compliance and guidance material to support the Part-IS regulatory package implementation' on 16 March 2023 at the EASA premises in Cologne. The workshop aimed at providing insights for a more informed commenting of the material. No comments have been collected during the workshop.

EASA reviewed the comments received and duly considered them. More information is provided in Section 2.5 of this document.

6 https://www.easa.europa.eu/en/document-library/notices-of-proposed-amendment/focused-consultations/npa-2023-102

2. In summary — why and what

2.1. Why we need to act — issue/rationale

Commission Implementing Regulation (EU) 2023/203 and Commission Delegated Regulation (EU) 2022/1645 lay down rules for the identification and management of information security risks in aviation organisations and aviation competent authorities, including EASA. The Decisions now issued provide AMC & GM for both the Implementing and the Delegated Commission Regulations, in order to facilitate their timely and harmonised application in the EASA Member States.

For the description of the issue that the Part-IS regulatory package addresses, see Opinion No 03/2021 'Management of information security risks'[7].

2.2. Assessment of the issue

For the assessment of the issue that the Part-IS regulatory package addresses, see Opinion No 03/2021 'Management of information security risks'.

2.3. Who is affected by the issue

For the description of the stakeholders affected by the issue, see Opinion No 03/2021 'Management of information security risks'.

2.4. What we want to achieve — objectives

The overall objectives of the EASA system are defined in Article 1 of the Basic Regulation. The regulatory material issued with these Decisions is expected to contribute to achieving these overall objectives by addressing the issue described in Section 2.1.

More specifically, through these Decisions, EASA intends to facilitate the timely and harmonised application of the Part-IS regulatory package.

2.5. What are the stakeholders' views

During the focused consultation of the Advisory Bodies, FAA, TCCA, CAA Israel and ANAC, a total number of 835 comments from 26 different stakeholders were received on NPA 2023-102. These were distributed as shown in Figure 1.

7 https://www.easa.europa.eu/en/document-library/opinions/opinion-032021

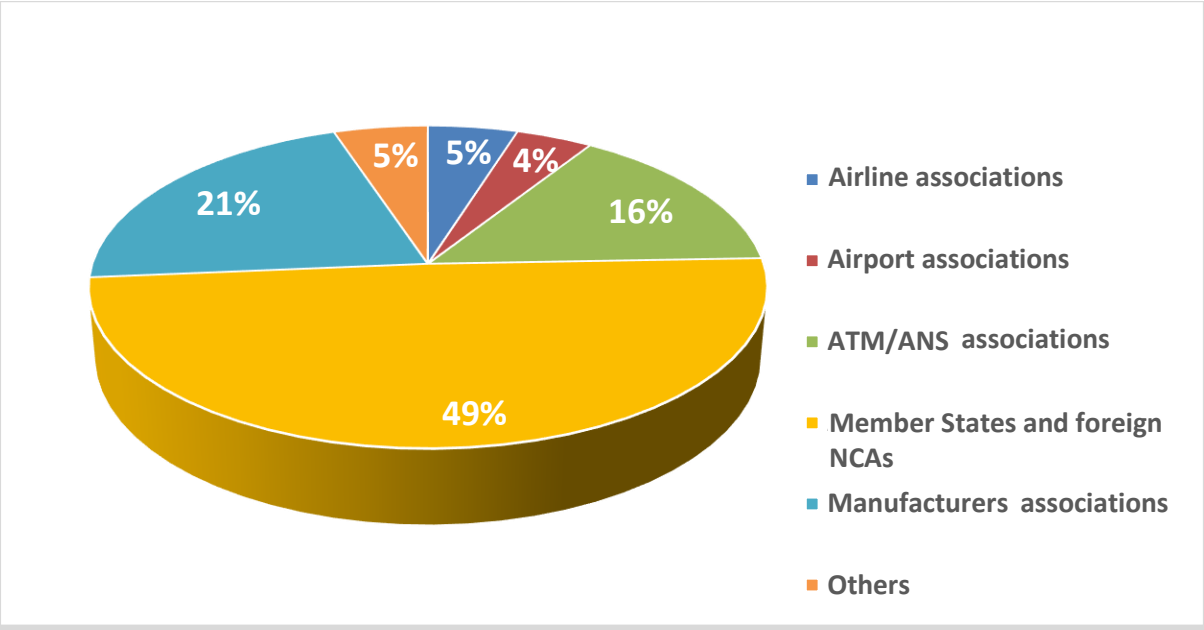

Figure 1: Distribution of comments per stakeholder group

The majority of the comments was related to the content of GM with a total of 62 %, while the comments on the AMC reached 38 % of the total comments received as shown in Figure 2. It has to be taken into account that due to the explanatory nature of GM, more content is provided with the intent of being used as guidance by stakeholders. This resulted in more material, in terms of quantity, to be commented, compared to the AMC.

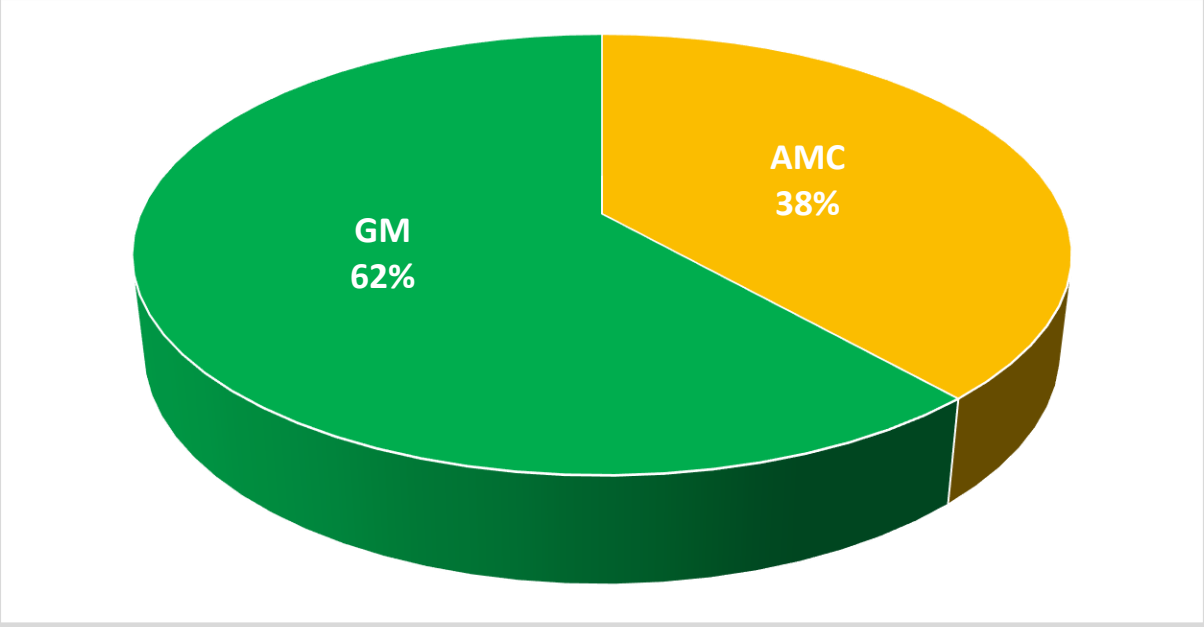

Figure 2: Distribution of comments on AMC and GM

The major comments, related considerations, and how they were addressed by EASA are summarised hereafter. Due to the similarity of the requirements on authorities with those on the organisations, in the scope of both the Implementing Regulation and the Delegated Regulation, the comments received in relation to certain topics have been grouped to better highlight the identified areas of interest and to provide an overview of the changes initiated by the comments received. Therefore, changes that were suggested and have been introduced in the AMC or GM to the authority requirements (ARs) have been also implemented in the organisation requirements (ORs) when those points were of a general nature. Figure 3 shows the distribution of the comments per area.

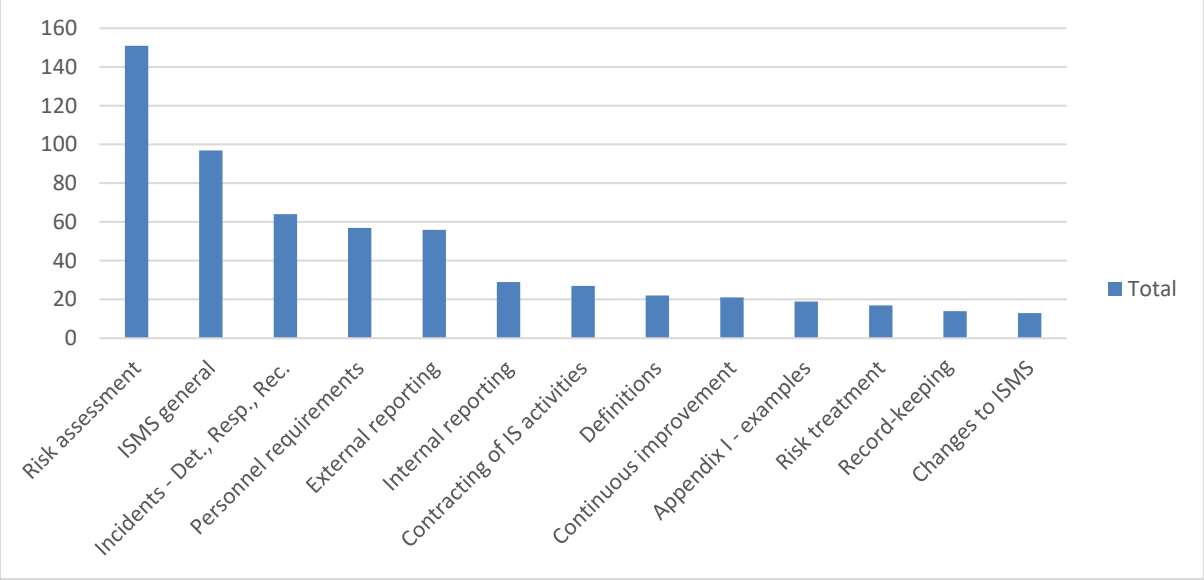

Figure 3: Distribution of comments per area

The above titles/data labels correspond to the following areas of the AMC & GM:

— Information security risk assessment (IS.I/D.OR.205 and IS.AR.205)
— Information security management system (ISMS) (IS.I/D.OR.200 and IS.AR.200)
— Information security incidents — detection, response and recovery (IS.I/D.OR.220 and IS.AR.215)
— Personnel requirements (IS.I/D.OR.240 and IS.AR.225)
— Information security external reporting scheme (IS.I/D.OR.230)
— Information security internal reporting scheme (IS.I/D.OR.215)
— Contracting of information security management activities (IS.I/D.OR.235 and IS.AR.220)
— Definitions (GM1 Article 3)
— Continuous improvement (IS.I/D.OR.260 and IS.AR.235)
— Examples of threat scenarios with a potential harmful impact on safety (Appendix I)
— Information security risk treatment (IS.I/D.OR.210 and IS.AR.210)
— Record-keeping (IS.I/D.OR.245 and IS.AR.230)
— Changes to the information security management system (IS.I/D.OR.255)

As it can be seen, a large number of comments have been received in the areas of the information security risk assessment as well as for the guidance material aiming to support the implementation of the information security management system (ISMS).

Regarding the risk assessment, the comments triggered a series of changes including the modification of the relevant AMC material regarding the scope of the risk identification and the risk assessment review. Additionally, more guidance has been provided in the GM with the aim of facilitating the organisations during the risk assessment implementation process. In this context, a set of examples of threat scenarios was provided in Appendix I that in turn received a number of comments by the stakeholders. This resulted in updating the indicative list of the threat scenarios by introducing a few more examples with a potential harmful impact on safety as well as by reviewing the editorial layout of this section.

The comments on the ISMS were mainly focused on the general guidance provided for the successful implementation of an ISMS. The comments received resulted in providing further clarifications about risk appetite considerations and the relation of Part-IS with existing information security management systems, leading to further highlighting and elaborating on the notion of aviation safety risks that drive the ISMS provisions of Part-IS.

On the detection of, response to and recovery from information security incidents, following the comments received, further clarification has been provided on the use of certain terms on the handling of incidents, and editorial changes were introduced for consistency purposes.

Comments were also received regarding the personnel requirements where further updates have been introduced on the appointment of the responsible person(s) and the establishment of trustworthiness for personnel having access to information systems and data subject to the rule.

Furthermore, the comments received on the information security external reporting scheme resulted in updating the AMC and GM to provide additional guidance on the relation with other reporting requirements while the text was further edited accordingly under this prism.

Other notable areas where a few comments were collected included the information security internal reporting scheme, resulting mainly in a few updates on the relationship between internal and external reporting, the contracting of information security management activities, in which further clarifications have been provided, and GM1 Article 3 ‘Definitions’, resulting in updating the list and introducing new terms or updating the description of existing ones to better represent their use in the AMC & GM to Part-IS.D.OR of Commission Delegated Regulation (EU) 2022/1645 as well as in the AMC & GM to Part-IS.AR and Part-IS.I.OR of Commission Implementing Regulation (EU) 2023/203. Last but not least, the continuous improvement area has been updated to provide more clarifications on the existing maturity models and levels, while the information security risk treatment, the record-keeping and the changes to the information security management system received a number of comments, resulting in updating the material to align the terminology used throughout the AMC & GM and to make it more concise where necessary.

The rest of the comments were distributed among other thematic sections of the regulatory material.

3. What are the expected benefits and drawbacks of the regulatory material

No additional impacts have been identified compared to those created by the Regulations and described in Opinion No 03/2021 'Management of information security risks'. Overall, the provision of AMC and GM is beneficial in supporting the timely and harmonised application of the rule.

4. Monitoring and evaluation

The usefulness of the AMC & GM to Commission Regulations (EU) 2022/1645 and 2023/203 will be monitored through standardisation and oversight activities.

Moreover the AMC & GM will be monitored in the frame of the implementation support task (IST.0001).

5. Proposed actions to support implementation

Under IST.0001 ‘Supporting the implementation of the IS management system (ISMS) by industry and NCAs’ described in Volume II of the EPAS for 2023–2025, EASA will:

— set up dedicated thematic workshops;

— support NCAs and organisations in the development of competence building / training for the implementation of the Part-IS regulatory package and the relevant oversight;

— set up a dedicated task force with volunteer NCAs to jointly discuss and address the challenges linked with the Part-IS regulatory package implementation;

— carry out pilot projects with volunteer organisations to implement the Part-IS regulatory package ahead of the applicability date.

6. References

The following (non-exhaustive) list includes regulations, internationally recognised standards in the field of information security, including standards with a specific focus on the aviation domain, as well as well-established frameworks in the field that have been considered during the development of these Decisions:

— Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 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 (EU) No 139/2014 and amending Commission Regulations (EU) No 748/2012 and (EU) No 139/2014

— Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 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 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664, and for competent authorities covered by Commission Regulations (EU) No 748/2012, (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340 and (EU) No 139/2014, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664 and amending Commission Regulations (EU) No 1178/2011, (EU) No 748/2012, (EU) No 965/2012, (EU) No 139/2014, (EU) No 1321/2014, (EU) 2015/340, and Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664

— ISO 27000 Series on ‘information security management systems (ISMS)’ standards

— EUROCAE ED-200 Series on ‘information security in aviation’ standards

— NIST Cybersecurity Framework (NIST CSF) V1.1 and NIST SP-800 Rev.1