Acceptable Means of Compliance and Guidance Material to the Articles of Commission Delegated Regulation (EU) 2022/1645 and Commission Implementing Regulation (EU)2023/203

Issue 1

12 July 2023[1]

[1] For the date of entry into force of this Issue, kindly refer to ED Decision 2023/008/R at the Official Publication of EASA.

TABLE OF CONTENTS

AMC AND GM TO THE ARTICLES OF COMMISSION DELEGATED REGULATION (EU) 2022/1645 AND COMMISSION IMPLEMENTING REGULATION (EU) 2023/203

GM1 Article 1 — Subject matter

When taking measures under this Regulation, affected entities — irrespective of their size — are encouraged to ensure that the measures they take are proportionate to the nature and safety risk of their activities.

GM1 Article 3 — Definitions

For the sake of common understanding, the following is a description of the terms used 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:

Assessment	In the context of management system performance monitoring, continuous improvement and oversight, it refers to a planned and documented activity performed by competent personnel to evaluate and analyse the achieved level of performance, effectiveness and maturity, as well as compliance in relation to the organisation's policy and objectives. *Note: An assessment focuses on required outcomes and the overall performance, looking at the organisation as a whole. The main objective of the assessment is to identify the strengths and weaknesses to drive continuous improvement.* *Remark: For 'risk assessment', please refer to the definition below.*
Attack vector (or attack path)	The path, interface, and actions by which an attacker executes an attack, as defined in EUROCAE ED-202.
Audit	It refers to a systematic, independent, and documented process for obtaining evidence, and evaluating it objectively to determine the extent to which requirements are complied with. *Note: Audits may include inspections.*
Competency	It is a combination of individual skills, practical and theoretical knowledge, attitude, training, and experience.
Correction	It is the action to eliminate a detected non-compliance.

Corrective action	It is the action taken to eliminate or mitigate the root cause(s) and prevent the recurrence of an existing detected non-compliance or other undesirable conditions or situations. Proper determination of the root cause(s) is crucial for defining effective corrective actions to prevent reoccurrence.
Deficiency	It is as a deviation from compliance with or a non-fulfilment of any requirement or objectives, either from a regulatory or an organisation's perspective, either completely or partially.
Experience	It is the fact or state of having been affected by or gained knowledge and skills through observation, participation or doing.
Functional chain	The concept of functional chain dictates that information security risks are shared along organisations due to their respective interfaces, such as supplier-customer relationships. Safety effects caused by information security threats primarily materialise at aircraft level, originating upstream of the aircraft. In the functional chain concept, each organisation assesses its information security risks, which it may not be able to address and hence may expose other organisations to risks. It should pass related information to the immediate partner(s) downstream for well-informed risk management purposes and to ensure that the whole chain is adequately protected, even when no organisation has full visibility or control.
Hazard	It is a condition or an object with the potential to cause or contribute to an aircraft incident or accident.
Information security control	It is a measure that reduces risk.
Intentional unauthorised electronic interaction	It refers to the deliberate act of engaging in electronic activities or communications (e.g. access to, or modification of, computer systems, networks, or data) without proper authorisation or permission and with the intent to disclose sensitive information, modify data, disrupt normal operations, or deny access to legitimate users.
Just culture	It means a culture in which front-line operators or other persons are not punished for actions, omissions or decisions taken by them that are commensurate with their experience and training, but in which gross negligence, wilful violations and destructive acts are not tolerated, as defined in Article 2 of Regulation (EU) No 376/2014[2].

[2] 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) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0376&qid=1669377456448).

Knowledge	Content of information needed to perform adequately in the job at an acceptable level, usually obtained through formal education and on-the-job experience. This knowledge is necessary for job performance but is not sufficient on its own.
Management (activity)	In the general organisational context, it refers to the activities aimed at directing, controlling, and continually improving the organisation within appropriate structures. In the context of Commission Delegated Regulation (EU) 2022/1645 and Commission Implementing Regulation (EU) 2023/203 it means, more specifically, the supervision and making of decisions necessary to achieve the organisation's safety and information security objectives.
Management system	It refers to a set of interrelated or interacting system elements to establish policies, objectives and processes to achieve those objectives, where the system elements include the organisational structure, roles and responsibilities, planning and operations.
Risk assessment	It is an evaluation that is based on engineering and operational judgement and/or analysis methods in order to establish whether the achieved or perceived risk is acceptable.
Risk register	It refers to a physical or digital means of documentation used as a risk management tool that acts as a repository for all identified risks and contains additional information about each risk, such as the nature of the risk, mitigation measures, ownership, status, etc.
Safety	It refers to the state in which risks associated with aviation activities, related to, or in direct support of the operation of aircraft, are reduced and controlled to an acceptable level, as defined in ICAO Annex 19.
Safety risk	It refers to the predicted likelihood and severity of the consequences or outcomes of a hazard. Note: The term 'likelihood' is used instead of the term 'probability' to reflect a subjective analysis of the possibility of occurrence rather than a purely statistical assessment.