SmartSuite

Framework / Cybersecurity / Other

EASA Part-IS – Regulation (EU) 2023/203

EASA Part-IS (Regulations (EU) 2023/203 and 2022/1645) requires aviation organizations to run an ISMS, manage safety-related information security risk and report incidents within 72 hours.



What it is

Part-IS is the European Union rule that requires aviation organizations and the authorities that oversee them to manage information security risks that could affect aviation safety. It is set out in Commission Implementing Regulation (EU) 2023/203 and Commission Delegated Regulation (EU) 2022/1645, and it applies from February 22, 2026 for most organizations under 2023/203 and from October 16, 2025 for those under 2022/1645.

At a glance

PUBLISHER
European Commission (regulations); EASA (AMC and GM)

TYPE
Regulation

VERSION
Implementing Regulation (EU) 2023/203 (Part-IS.AR, Part-IS.I.OR), as amended by (EU) 2023/1769, 2024/1109 and 2025/2293; Delegated Regulation (EU) 2022/1645 (Part-IS.D.OR)

EFFECTIVE
February 22, 2026 (Implementing Regulation (EU) 2023/203); October 16, 2025 (Delegated Regulation (EU) 2022/1645)

DOMAIN
Cybersecurity

FAMILY
Other

REGION
European Union

INDUSTRY
Aerospace & Defense

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: easa.europa.eu/en/regulations/information-security

Why it matters

- **One ISMS requirement across the sector** Annex II (Part-IS.I.OR) applies to most organizations, with Part-IS.D.OR in Regulation 2022/1645 for design, production and aerodrome organizations, so the sector shares one standard.
- **Risk is measured by safety impact** Risks are classified by the chance of the threat scenario and the severity of its safety consequences (IS.I.OR.205(c)).
- **A fixed reporting clock** Reportable incidents and vulnerabilities go to the competent authority within 72 hours of the organization knowing about them (IS.I.OR.230(c)(2)).
- **Top management is accountable** The accountable manager must have the corporate authority to resource compliance and promote the policy (IS.I.OR.240(a)).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports EASA Part-IS (EU 2023/203)

ISMS Requirement Library

Map each IS.I.OR.200 to .260 requirement to an owner, procedure and evidence, with the accountable manager's approval.

Safety-Linked Risk Register

Record exposed elements, interfaces with other organizations, risk level and treatment, and review dates when changes or incident lessons occur (IS.I.OR.205 and .210).

Incident Detection and Reporting

Track events through detection, response and recovery, and time the 72-hour report and the follow-up to the competent authority (IS.I.OR.220 and .230).

Contracted Activity Oversight

Log organizations that perform ISMS activities for you, the contract terms and the oversight evidence (IS.I.OR.235).

Records and Retention

Keep risk assessments, incident records and personnel qualification records with the five-year and three-year retention rules (IS.I.OR.245).

Authority Findings and Improvement

Record findings from competent authority audits, corrective actions and the continuous improvement cycle with dates (IS.I.OR.225 and .260).

Common framework mappings

CIS Controls v8.1 | GDPR | ISO 27001:2022 | ISO 27002:2022 | ISO 27701 | NIS2 (EU 2022/2555) | NIST CSF 2.0 | NIST 800-53 Rev.5

Official resources

EASA Part-IS — Information Security Regulation (EU) 2023/203

Defines mandatory cybersecurity and information security requirements for EU civil aviation organizations.

easa.europa.eu/en/regulations/information-security

EASA Guidance Material on Information Security

Provides implementation guidance supporting EASA Part-IS requirements for aviation entities.

easa.europa.eu/en/acceptable-means-compliance-and-guidance-material-group/part-isior-information-security

EASA Security Controls Framework

Outlines the security controls required under EASA Part-IS for compliance.

easa.europa.eu/en/document-library/easy-access-rules/easy-access-rules-information-security-regulations-eu-2023203

EASA Cybersecurity Risk Management Guidelines

Describes the approach to managing cybersecurity risks in the aviation sector.

easa.europa.eu/en/the-agency/faqs/information-security-part

Frequently asked questions

Who must comply with EASA Part-IS?

Maintenance organizations, continuing airworthiness management organizations, air operators, approved training organizations, aero-medical centers, simulator operators, air navigation service providers, U-space providers and system designers under Regulation 2023/203 (Article 2), plus design and production organizations and aerodrome operators under Delegated Regulation 2022/1645. Competent authorities follow Part-IS.AR.

When does Part-IS apply?

Regulation 2023/203 applies from February 22, 2026 (January 1, 2026 for the EGNOS air navigation service provider). Delegated Regulation 2022/1645 applies from October 16, 2025. Ground handling organizations come in from March 27, 2031.

What must an organization report and how quickly?

Any information security incident or vulnerability that may represent a significant risk to aviation safety is reported to the competent authority. A notification is made as soon as it is known, a report within 72 hours, and a follow-up report once recovery and prevention actions are identified (IS.I.OR.230).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

Does Part-IS require ISO 27001 or NIST?

No. EASA's guidance says Part-IS does not require a specific framework such as ISO or NIST, although certifications can serve as supporting evidence if they cover the Part-IS scope. The ISMS may be integrated with other management systems (IS.I.OR.200(d)).

Can an organization be exempt from the ISMS requirements?

Yes, if its competent authority approves it, based on a documented risk assessment showing its activities, facilities, resources and services pose no information security risk with a potential impact on aviation safety (IS.I.OR.200(e)).

License included / downloadable: Yes The regulations are EU law published in the Official Journal, and EASA publishes the Easy Access Rules and AMC and GM free; they are included with the platform for reference.

Full framework page and mappings: smartsuite.com/frameworks/easa-part-is-information-security-regulation-eu-2023-203

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.