SmartSuite

Framework / Cybersecurity / Other

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

EASA Part-IS is an EU regulation requiring civil aviation organizations to implement cybersecurity measures to protect aviation information and operations.

What it is

EASA Part-IS — Information Security Regulation (EU) 2023/203 is a European Union regulation that establishes mandatory cybersecurity and information security requirements for civil aviation organizations. Its primary purpose is to enhance the protection of information and systems supporting aviation safety, ensuring resilience against cyber threats and minimizing risks to critical aviation operations.

Issued by the European Union Aviation Safety Agency (EASA), Part-IS applies to a wide range of organizations in the civil aviation sector, including air carriers, maintenance organizations, and airport operators within the EU. The regulation sets out comprehensive requirements covering cybersecurity risk management, incident reporting, security controls, and governance to safeguard aviation-specific information assets and operational infrastructure.

At a glance

PUBLISHER European Union Aviation Safety Agency (EASA)	TYPE Regulation	VERSION Commission Implementing Regulation (EU) 2023/203
EFFECTIVE 2023	DOMAIN Cybersecurity	FAMILY Other
REGION European Union	INDUSTRY Aerospace & Defense	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

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

Why it matters

- **Strengthen cybersecurity governance** Promote consistent security leadership by integrating information security into organizational policies, management processes, and oversight structures.
- **Enhance regulatory alignment** Enable organizations to meet EU aviation cybersecurity requirements, reducing gaps in compliance and supporting ongoing regulatory reporting obligations.
- **Improve incident detection and response** Facilitate robust monitoring and escalation procedures, allowing faster identification and containment of cyber incidents impacting aviation operations.
- **Protect sensitive operational data** Implement targeted controls that help secure flight, passenger, and operational data critical to safety and business continuity.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

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

IS Governance and Accountability

Track roles, policies, oversight actions, and reporting across the program.

Part-IS Risk Assessments and Mitigations

Run Part-IS risk assessments and manage mitigations with approvals and evidence.

Control Library and Evidence Hub

Map requirements to controls and centralize proof of implementation and operation.

Incident and Escalation Workflows

Manage incidents with timelines, decisions, and cross-team coordination.

Supplier and Outsourcing Oversight

Track third-party requirements, due diligence, and monitoring evidence.

Regulatory Readiness Reporting

Report posture, gaps, and improvement actions for audits and oversight.

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

What is EASA Part-IS used for?

EASA Part-IS establishes mandatory information security requirements for civil aviation organizations in the European Union. Its primary purpose is to enhance the cybersecurity resilience of aviation operations, protect critical information assets, and minimize risks from cyber threats impacting aviation safety.

Is compliance with EASA Part-IS mandatory?

Yes, compliance with EASA Part-IS is mandatory for the covered entities. All organizations within its defined scope must implement the specified information security controls and processes to meet regulatory obligations under Regulation (EU) 2023/203.

Which organizations are in scope for EASA Part-IS?

EASA Part-IS applies to civil aviation organizations operating within the EU, including air carriers, maintenance organizations, airport operators, and other entities supporting aviation safety. Service providers and suppliers with access to critical aviation information or systems may also be required to comply.

What cybersecurity controls are required by EASA Part-IS?

The regulation requires a comprehensive set of cybersecurity controls, including risk assessments, asset management, access control, governance, incident reporting, supply chain security, and business continuity processes. Organizations must tailor these controls to address the specific risks facing their aviation operations.

 · © 2026 SmartSuite Inc. All rights reserved.

How does the implementation process for EASA Part-IS work?

Implementation involves integrating regulatory requirements into existing information security management systems (ISMS), appointing accountable personnel, conducting regular vulnerability and risk assessments, and aligning operational practices with the regulation. Ongoing monitoring, staff training, and internal audits are also necessary for effective execution.

How does EASA Part-IS relate to other information security frameworks?

EASA Part-IS is aligned with international standards like ISO/IEC 27001, but it includes sector-specific controls tailored for aviation. Organizations often map EASA requirements to other frameworks to streamline compliance across regulatory regimes.

What are the ongoing compliance obligations under EASA Part-IS?

Ongoing obligations include regular security risk reviews, timely incident reporting to competent authorities, continuous monitoring of security measures, and maintaining up-to-date documentation and evidence of compliance. Audits by regulators or independent assessors may also be required.

How would SmartSuite support EASA Part-IS?

SmartSuite supports EASA Part-IS compliance by providing tools for risk tracking, centralized control management, and automated evidence collection. It enables compliance teams to track requirements, manage incident reports, and prepare for audits with readiness checklists and reporting dashboards, ensuring effective oversight and governance of information security obligations.

License included / downloadable: Yes EASA Part-IS is a European Union regulation and is publicly available through official EU regulatory publications.

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

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.