

UK CAA CAP 1850

UK CAP 1850 provides guidance for cybersecurity oversight of UK aviation systems to ensure safety and resilience.



What it is

UK CAP 1850 — Cybersecurity Oversight for Aviation Systems is a regulatory framework that helps organizations in the aviation sector manage cybersecurity risks and enhance the protection of critical aviation systems. The framework establishes structured guidance for identifying, mitigating, and monitoring cybersecurity threats to ensure the resilience and safety of aviation operations.

Published by the UK Civil Aviation Authority (CAA), CAP 1850 is intended for aviation operators, airports, and service providers responsible for the security of operational technologies and information systems. It addresses areas such as cybersecurity controls, risk management, incident response, and compliance oversight within the context of aviation-specific regulatory requirements.

At a glance

PUBLISHER Civil Aviation Authority (CAA)	TYPE Regulation	VERSION 2
EFFECTIVE 19 August 2020	DOMAIN Cybersecurity	FAMILY Other
REGION United Kingdom	INDUSTRY Aerospace & Defense	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: <https://www.caa.co.uk/our-work/publications/documents/content/cap1850/>

Why it matters

- **Strengthen cybersecurity governance** Promote clear responsibility and accountability for cybersecurity management across aviation operations and supporting technology environments.
- **Enhance regulatory alignment** Enable organizations to comply with UK aviation and cybersecurity regulations through clearly defined requirements and documentation.
- **Improve risk management practices** Support robust identification and mitigation of threats specific to aviation systems, helping reduce exposure to operational and safety risks.
- **Increase audit readiness** Document and formalize cybersecurity controls, making it easier to demonstrate compliance during regulatory reviews or external audits.

How SmartSuite supports CAP 1850

Aviation Security Control Framework

Structure CAP 1850 requirements with ownership, scope, and implementation tracking across systems.

Risk Assessment and System Classification

Link cybersecurity risks to aviation systems and prioritize controls based on criticality.

Governance, Policy, and Oversight Management

Centralize policies, procedures, and accountability aligned to aviation regulatory expectations.

Aviation System Access and Operational Safeguards

Manage authentication, access, and operational safeguards across aviation systems.

Aviation Cybersecurity Incident Reporting

Track cybersecurity incidents and manage reporting obligations to aviation authorities.

CAP 1850 Compliance Monitoring and Regulatory Reporting

Provide dashboards showing control coverage, risk posture, and CAP 1850 compliance readiness.

Common framework mappings

CIS Controls v8.1

NIS2 (EU 2022/2555)

ISO 27001:2022

NIST CSF 2.0

NIST 800-53 Rev.5

SOC 2

Cyber Essentials

Official resources

Cyber Assessment Framework (CAF) for Aviation – CAP 1850

Provides guidance for completing the Cyber Assessment Framework tailored to aviation operations.
caa.co.uk/publication/download/17540

CAP 1849: Cyber Security Critical Systems Scoping Guidance

Defines how to identify and document critical systems in aviation for cybersecurity assessment.
caa.co.uk/our-work/publications/documents/content/cap1849

CAP 1753: The Cyber Security Oversight Process for Aviation

Describes the CAA's primary oversight process for assessing cybersecurity in safety-critical aviation systems.
caa.co.uk/publication/download/21585

Frequently asked questions

What is UK CAP 1850 used for?

UK CAP 1850 provides regulatory guidance for the cybersecurity oversight of aviation systems in the United Kingdom. The framework establishes baseline requirements to safeguard aviation-critical infrastructure and ensure compliance with the UK Civil Aviation Authority's cybersecurity objectives.

Is UK CAP 1850 mandatory for aviation organizations?

UK CAP 1850 is a mandatory framework for regulated entities within the UK's aviation sector, such as airports, airlines, and air navigation service providers. Compliance is required to demonstrate adherence to the UK CAA's cybersecurity obligations and to maintain regulatory approval for operations.

What systems and organizations are in scope for UK CAP 1850?

The framework applies to organizations and systems considered essential to safe and secure aviation operations, including those supporting air traffic management, airport operations, aircraft, and supporting IT infrastructure. Both direct service providers and critical third-party vendors may be subject to CAP 1850 oversight depending on their operational impact.

What key requirements or artifacts are specified by UK CAP 1850?

UK CAP 1850 requires organizations to implement robust cybersecurity governance, conduct risk assessments, document risk treatment plans, and establish incident response processes. Organizations must maintain records of security controls, periodic reviews, and corrective actions, as well as evidence of workforce cybersecurity awareness.

How is UK CAP 1850 implemented in practice?

Implementation involves conducting an initial cybersecurity risk assessment, establishing policies and procedures aligned with CAP 1850 requirements, and integrating cybersecurity into safety management processes. Organizations must routinely reassess risks, update documentation, and evidence ongoing compliance to the UK CAA.

How does UK CAP 1850 relate to other security frameworks?

UK CAP 1850 aligns with international standards such as ICAO Annex 17 and ISO 27001, but contains specific controls tailored for the aviation sector under UK oversight. It complements, rather than replaces, other sector frameworks, and harmonization is encouraged for airlines and operators subject to multiple jurisdictions.

What ongoing compliance activities are required under UK CAP 1850?

Organizations must perform regular cybersecurity audits, maintain up-to-date risk assessments, conduct incident simulations, and report significant incidents to the UK CAA. Continuous monitoring and periodic evidence submissions are required to demonstrate sustained compliance.

How would SmartSuite support UK CAP 1850 — Cybersecurity Oversight for Aviation Systems?

SmartSuite can help organizations manage UK CAP 1850 by centralizing risk tracking, mapping controls to regulatory requirements, and facilitating the collection and storage of compliance evidence. It supports task assignment for remediation, enables ongoing audit readiness, and produces compliance reports that streamline engagement with regulatory bodies.

License included / downloadable: Yes Published by the UK Civil Aviation Authority (CAA), CAP 1850 is publicly available as a free PDF on the CAA website. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/uk-cap-1850-cybersecurity-oversight-for-aviation-systems