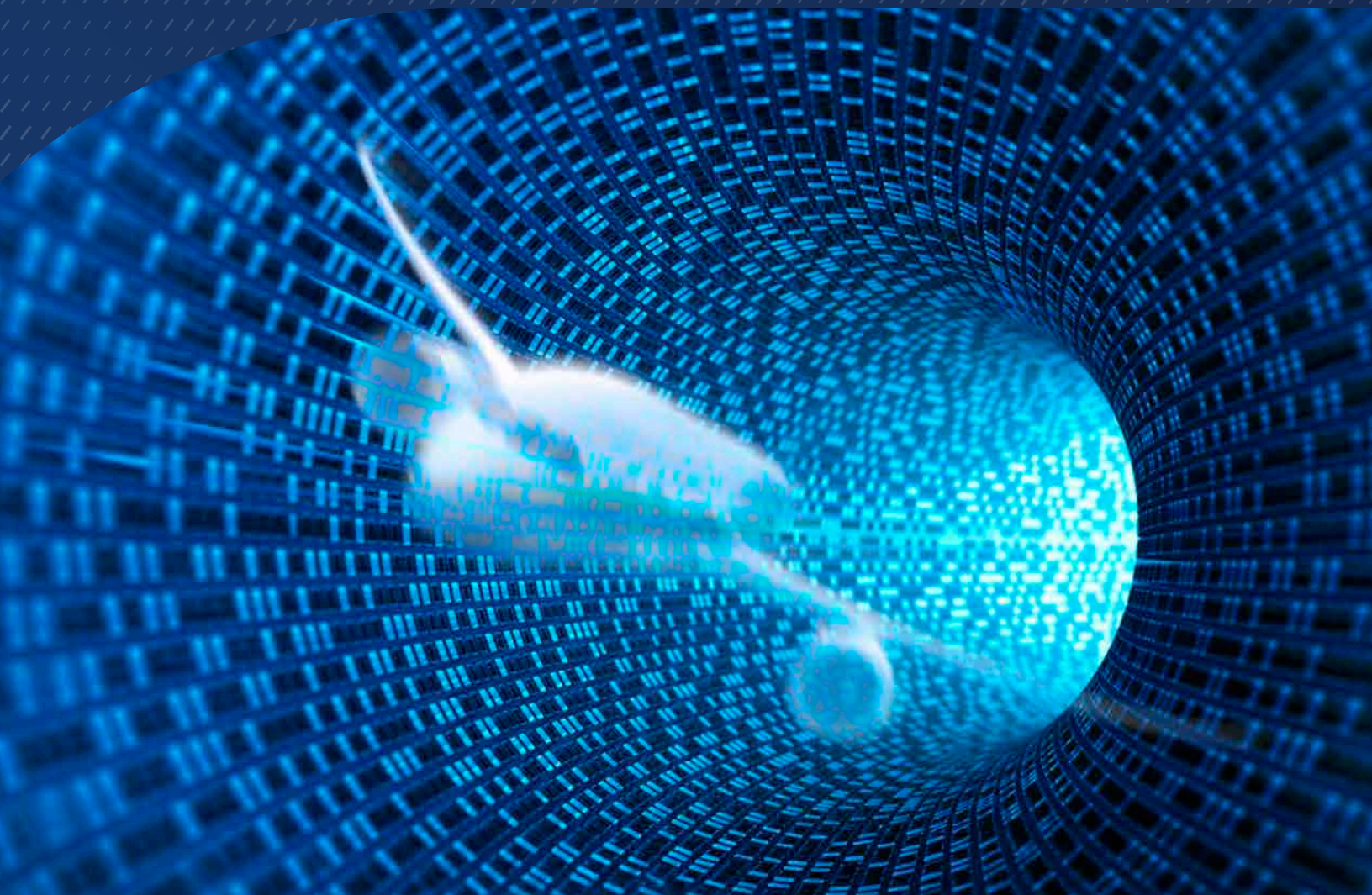
BOEING

Service above and beyond

# Boeing SkyGuard

## Securing tomorrow's skies — cyber resilience with SkyGuard



# Boeing SkyGuard

## Securing tomorrow's skies — cyber resilience with SkyGuard

In an era where connectivity transforms aircraft and ground systems, cybersecurity must be strategic, not reactive.

Boeing provides pragmatic frameworks for building resilient, OEM-agnostic ecosystems that detect anomalies, prioritize risks, and enable rapid mitigation across aircraft, flight operations, IT, and ground operating systems.

Learn more about regulatory imperatives such as FAA and EASA guidance and those from major regional civil aviation authorities, including: GCAA (UAE) aligned with NESA IA Standards and TDRA Aviation Cyber guidance, GACA (Saudi Arabia) aligned with NCA ECC and CCC under Vision 2030, CAAC (China), DGCA (India), CAAS (Singapore) aligned with the CSA Cybersecurity Code of Practice for CII Aviation sector, and JCAB (Japan), within a broader push for GCC cyber harmonization and sovereign cyber resilience across the region.

# What is SkyGuard?

SkyGuard is Boeing's end-to-end cyber resilience offering for aviation ecosystems worldwide. It combines policy alignment, intelligent analytics, continuous monitoring, and operational integration to deliver OEM-agnostic protection across aircraft systems, flight operations, IT, and ground infrastructure.

## Why SkyGuard matters

- Holistic protection across airborne and ground attack surfaces
- Aligned with FAA, EASA, and other global regulatory guidance for aviation cybersecurity
- AI-driven analytics that turn telemetry and logs into prioritized, actionable intelligence
- Playbooks and governance models designed for safety-critical, regulated environments
- Rapid detection → prioritized response → controlled mitigation to preserve operations and reputation

# How SkyGuard aligns to NIST cybersecurity and risk frameworks

| Framework | Description |
|---|---|
| Governance | Cross-organizational governance models, role-based decision authorities, and evidence chains that align safety and cybersecurity priorities. |
| Identify | Critical asset discovery, data-source mapping, and threat-surface analysis to build a complete inventory and risk baseline. |
| Protect | Controls for prevention and system hardening: segmentation, secure update processes, configuration management, identity and access management, and protective monitoring. |
| Detect | Anomaly detection and behavioral baselining for aircraft/embedded system telemetry and related sources. |
| Respond | Incident playbooks, escalation matrices, and orchestration of containment and mitigation actions tied to operational roles and safety procedures. |
| Recover | Restoration plans, forensics and evidence preservation, post-incident remediation, and continuous improvement to restore normal operations and reduce recurrence. |

# Why you should act

Through SkyGuard, Boeing provides a clear playbook for embedding cybersecurity into lifecycle processes, fostering cross-organizational collaboration, and leading cultural change so airlines can confidently scale digital innovation while protecting passengers, crews, and critical assets.

## Regulatory imperatives and compliance

Industry guidance increasingly requires proactive cybersecurity lifecycle integration, vulnerability management, and evidence of operational resilience. SkyGuard helps demonstrate compliance by embedding traceable controls, continuous evidence collection, and capability assessments mapped to regulatory controls and guidance..

SkyGuard delivers continuous detection, prioritized response, and regulator-ready evidence so your operations stay safe, compliant, and resilient.

In the EU, this includes EASA Part-IS (Reg. EU 2022/1645 and 2023/203), enforceable since 22 February 2026, where SkyGuard modules map directly to IS.D.OR.205 (risk assessment), IS.D.OR.215 (ISMM), IS.D.OR.230 (monitoring), and IS.D.OR.240 (continual improvement)

**Click here to request a SkyGuard briefing or proof of value today!**

# Comprehensive modular approach to NIST cybersecurity and risk frameworks

**Boeing SkyGuard offers a flexible, modular approach for every phase of the cybersecurity assessment lifecycle:**

## Discovery and baseline risk

Airline/operator asset inventory and security categorization, cybersecurity risk assessment, regulatory gap analysis, data sources, and initial threat modelling.

## Proof of value deployment

Integrate key telemetry sources, tune analytics, run pilot detection and response exercises.

## Operationalization

Extend telemetry coverage, embed playbooks, integrate with ops tooling, stand up governance.

## Continuous improvement

Model refinement, periodic red team exercises, compliance reporting cadence, training cycles.

# Key highlights: SkyGuard

## Governance models that balance safety and efficiency

- **Joint safety/security council:** harmonized decision authority that aligns safety cases and risk tolerances.
- **Tiered escalation:** role-specific authority for response (flight ops, engineering, cyber-SOC, legal, communications).
- **Change control integration:** cybersecurity gates embedded into configuration management, software updates, and MRO workflows.

## AI-driven analytics: turning logs into action

- **Ingest:** multi-format logs and telemetry (avionics buses, maintenance systems, network devices, cloud services).
- **Normalize:** map disparate schemas into a unified model for correlation.
- **Analyze:** machine learning models detect anomalies, cluster events, and surface causal chains.
- **Act:** automatic prioritization and recommended mitigation actions integrated into operational workflows and ticketing.

# Trust a Proven Approach

SkyGuard sets you up for cybersecurity success. Bringing in years of Boeing best practices in both the commercial and military aviation fields, SkyGuard is your end-to-end consultancy solution for managing complex frameworks that enable and support:

- Necessary cybersecurity information to operators to ensure continued airworthiness (ANSOG & DO-355A/ED-204A)
- Management of cybersecurity incidents and events that impact aircraft safety (DO-392/ED-206)
- Development of aircraft information security operational concepts (ARINC 811)
- Operators to routinely report ANSP activity to Regulator, helping them from missing deadlines

## Key Outcomes

- Continuous detection and mean time to respond (MTTR) through prioritized alerts and automation
- Clear regulatory alignment and evidence packages for audits and reporting
- Reduced operational risk and minimized service disruptions during incidents
- Cross-functional collaboration that preserves safety while enabling digital growth

# Why partner with Boeing?

With nearly five decades of domain expertise, Boeing combines expert consulting with industry-leading software tools, providing pragmatic frameworks and building resilient cybersecurity solutions for airline, defense, and business aviation operators.

Discover how SkyGuard can help your organization embed cybersecurity across the aircraft lifecycle and operational estate. Contact Boeing Aviation Business Solutions Consulting to arrange a briefing, regulatory readiness assessment, or technical pilot.

> **Run operations, not investigations. Contain and resolve incidents without disrupting schedules — stand up SkyGuard**

## Contact Us

**Aviation Business Solutions — Cybersecurity and Digital Transformation**

Email: skyguard@boeing.com

services.boeing.com/skyguard

Service above and beyond

**Boeing Global Services Marketing**
P.O. Box 3707
Seattle, WA 98124-2207

services.boeing.com



14107 CA 04_26