AirCyber et BoostAerospace 2026 : Conformité Cybersécurité Aéronautique

> Guide AirCyber et BoostAerospace 2026 — référentiel cybersécurité aéronautique, questionnaire auto-évaluation, audit fournisseurs GIFAS et connexion NIS 2.

La filière aéronautique française est l'une des premières à avoir structuré un référentiel de cybersécurité sectoriel dédié à sa supply chain. AirCyber, programme initié par le GIFAS (Groupement des Industries Françaises Aéronautiques et Spatiales) en partenariat avec l'IHEDN (Institut des Hautes Études de Défense Nationale), vise à élever le niveau de maturité cyber de l'ensemble de la chaîne d'approvisionnement aéronautique française — des grands donneurs d'ordres (Airbus, Safran, Dassault, Thales) jusqu'aux PME et ETI sous-traitantes. En 2026, AirCyber s'est considérablement renforcé avec l'intégration de BoostAerospace — la plateforme collaborative de l'industrie aéronautique — comme vecteur de collecte et de validation des auto-évaluations. Sous la pression conjointe des donneurs d'ordres, des obligations NIS 2 pour les OSE du secteur, et de la norme DO-326A (cybersécurité des systèmes aéronautiques embarqués), la conformité AirCyber est devenue un critère d'éligibilité aux contrats aéronautiques en France. Ce guide présente le programme AirCyber dans son état 2026 : historique, questionnaire des 45 questions et niveaux de maturité, intégration BoostAerospace, articulation avec NIS 2 et DO-326A, exigences Airbus et Safran pour leurs fournisseurs, et roadmap de mise en conformité pour les PME de la supply chain.

À RETENIR

À retenir — AirCyber & BoostAerospace 2026

• AirCyber est le référentiel cybersécurité de la supply chain aéronautique française (GIFAS)

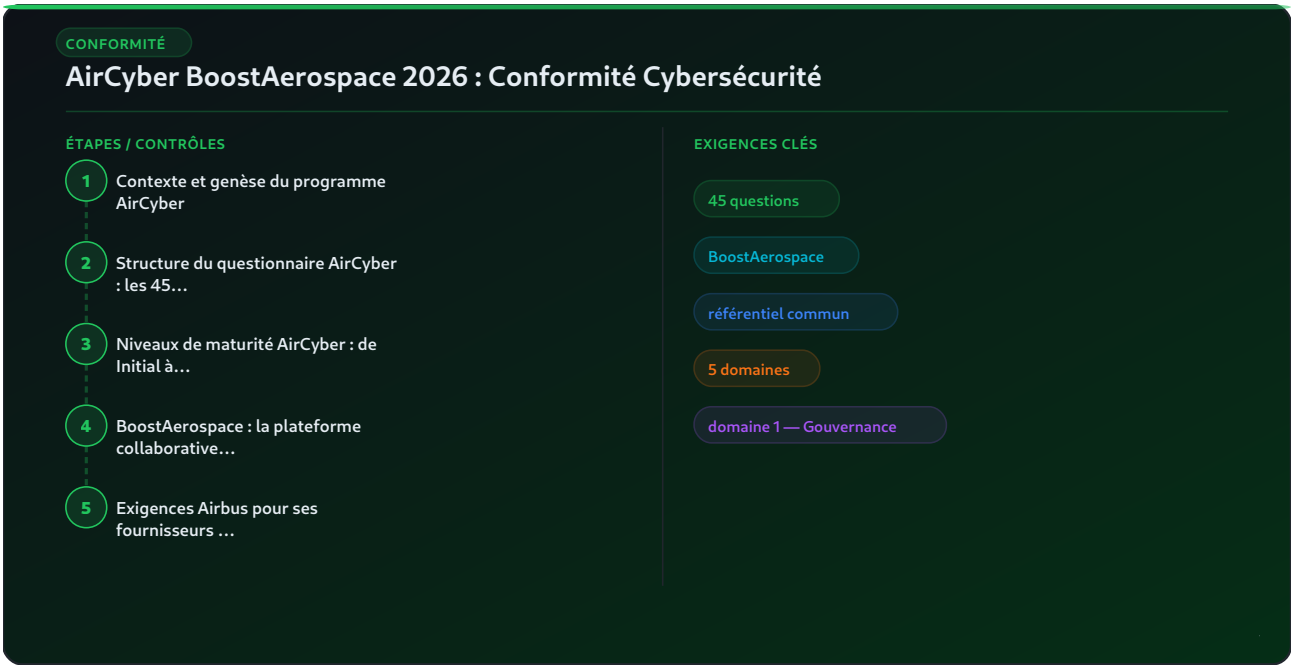
• **45 questions** structurées en 5 domaines évaluant la maturité cyber des sous-traitants

• **BoostAerospace** : plateforme de collecte et partage des auto-évaluations AirCyber entre donneurs d'ordres

• Niveaux 1 à 5 (Initial → Optimisé) — niveau 3 requis par Airbus et Safran pour les fournisseurs critiques

• Articulation NIS 2 : les OSE du secteur aéronautique sont soumis à NIS 2 ET à AirCyber simultanément

• **DO-326A** couvre la cybersécurité des systèmes aéronautiques embarqués — distinct d'AirCyber (systèmes IT des fournisseurs)



Contexte et genèse du programme AirCyber

Le programme AirCyber est né du constat que les grandes entreprises aéronautiques (Airbus, Safran, Dassault Aviation, Thales, ArianeGroup) avaient développé leurs propres référentiels de sécurité fournisseurs, créant une multiplication des questionnaires et des audits que les PME sous-traitantes devaient gérer en parallèle — avec des coûts et une charge administrative importants. L'objectif d'AirCyber était de créer un **référentiel commun**, reconnu par l'ensemble

des donneurs d'ordres de la filière, permettant à un fournisseur de réaliser une seule auto-évaluation partageable avec tous ses clients aéronautiques. Initié en 2019 sous l'égide du GIFAS, AirCyber s'est inspiré de démarches similaires dans d'autres secteurs : le CMMC (Cybersecurity Maturity Model Certification) dans la défense américaine, l'ENX TISAX dans l'automobile européenne. Le lancement officiel du programme avec son questionnaire de 45 questions date de 2020, avec une montée en charge progressive dans la supply chain sur 2021-2024. En 2026, plusieurs centaines d'entreprises françaises ont réalisé leur auto-évaluation AirCyber et partagé leurs résultats via BoostAerospace. L'IHEDN apporte une dimension de sensibilisation et de formation, notamment pour les dirigeants de PME qui ne perçoivent pas encore la cybersécurité comme un enjeu stratégique dans leur contexte industriel.

Structure du questionnaire AirCyber : les 45 questions en 5 domaines

Le questionnaire AirCyber est structuré en **5 domaines** couvrant les aspects fondamentaux de la cybersécurité organisationnelle et technique. Le **domaine 1 — Gouvernance** (environ 8 questions) évalue l'existence d'une politique de sécurité formalisée, la désignation d'un responsable sécurité, la sensibilisation des dirigeants, et l'intégration de la cybersécurité dans la stratégie d'entreprise. Le **domaine 2 — Protection** (environ 12 questions) couvre les contrôles techniques de base : gestion des accès et des identités, sécurité des postes de travail (antivirus/EDR, chiffrement), sécurité réseau (pare-feu, segmentation, Wi-Fi), et sécurité physique. Le **domaine 3 — Défense** (environ 10 questions) évalue la capacité de détection des incidents, la journalisation des accès, le monitoring réseau et les alertes de sécurité. Le **domaine 4 — Résilience** (environ 10 questions) couvre les sauvegardes, le plan de continuité, les procédures de reprise après incident, et la gestion des relations avec les prestataires. Le **domaine 5 — Cyber Supply Chain** (environ 5 questions) évalue la manière dont l'entreprise gère la cybersécurité de ses propres fournisseurs et sous-traitants. Chaque question reçoit un score de 0 à 4 selon le niveau de maturité de la pratique évaluée, et le score global détermine le niveau de maturité AirCyber de l'entreprise.

⚡ **Retour terrain**

J'ai réalisé un audit de conformité PCI-DSS pour un e-commerçant de taille moyenne. La surprise : leur prestataire de paiement gérait effectivement la conformité PCI côté serveur, mais les formulaires de carte côté client passaient par leurs propres serveurs via un JavaScript personnalisé — introduisant un scope PCI non déclaré. La remédiation a nécessité une migration vers un formulaire de paiement hébergé (redirect ou iFrame).

Niveaux de maturité AirCyber : de Initial à Optimisé

AirCyber définit **5 niveaux de maturité** cybersécurité inspirés du modèle CMMI (Capability Maturity Model Integration). Le **Niveau 1 — Initial** : les pratiques de sécurité sont ad hoc et réactives, sans documentation formelle. La sécurité est gérée au cas par cas en réponse à des incidents. Le **Niveau 2 — Répétable** : des pratiques de base sont en place et répétables mais non standardisées. Des procédures existent mais peuvent varier selon les individus. Le **Niveau 3 — Défini** : les processus de sécurité sont documentés, standardisés et suivis par l'ensemble de l'organisation. Un plan de sécurité est en place et mis à jour régulièrement. C'est le niveau minimum exigé par la plupart des donneurs d'ordres aéronautiques pour les fournisseurs critiques. Le **Niveau 4 — Géré** : la sécurité est mesurée et contrôlée via des indicateurs. Les décisions sont basées sur des données et des mesures objectives. Le **Niveau 5 — Optimisé** : la sécurité est en amélioration continue, avec des processus d'innovation et d'optimisation systématiques. La majorité des PME aéronautiques se situent actuellement entre les niveaux 1 et 2 — la montée vers le niveau 3, requis par les donneurs d'ordres, est l'objectif principal du programme AirCyber pour la période 2024-2027.

BoostAerospace : la plateforme collaborative de partage des évaluations

BoostAerospace est une plateforme collaborative créée par les grands donneurs d'ordres de l'industrie aéronautique (Airbus, Dassault, Safran, Thales) pour fluidifier les échanges de données non concurrentielles dans la filière. Dans le contexte AirCyber, BoostAerospace sert de **référentiel centralisé** pour les auto-évaluations des fournisseurs : un fournisseur remplit son questionnaire AirCyber une seule fois sur la plateforme, et peut le partager avec l'ensemble de ses clients donneurs d'ordres qui sont également membres de BoostAerospace. Ce mécanisme de "réponse unique, partage multiple" est le principal avantage d'AirCyber par rapport aux approches individuelles. L'accès à BoostAerospace est conditionné à une adhésion (environ 2 000 à 5 000 €/an selon la taille de l'entreprise) et à la signature d'une charte d'utilisation. Les auto-évaluations AirCyber sur BoostAerospace ne sont pas auditées automatiquement — elles sont déclaratives et s'inscrivent dans une logique de confiance initiale, avec des audits de vérification possibles par les donneurs d'ordres pour les fournisseurs critiques. La plateforme assure également la confidentialité : les données de sécurité d'un fournisseur ne sont partagées qu'avec les donneurs d'ordres auxquels il a explicitement accordé l'accès.

Exigences Airbus pour ses fournisseurs : SSCT et AirCyber

Airbus a développé son propre référentiel de cybersécurité fournisseurs — le **SSCT (Supplier Cybersecurity Technical Requirements)** — intégré dans ses conditions d'achat générales (General Procurement Conditions). En 2026, le SSCT impose aux fournisseurs d'Airbus un niveau minimum de maturité AirCyber et des contrôles techniques spécifiques. Les fournisseurs classifiés "Critical" par Airbus (accès aux données de conception, aux systèmes IT d'Airbus ou aux données Export Control) sont soumis aux exigences les plus strictes : niveau AirCyber 3 minimum, audit de cybersécurité possible par Airbus ou un prestataire mandaté, et reporting d'incidents cyber dans les 72 heures. Les fournisseurs "Major" sont soumis à un niveau AirCyber 2 minimum avec auto-évaluation validée sur BoostAerospace. Les fournisseurs "Standard" sont informés des exigences sans obligation d'audit. La classification des fournisseurs Airbus est réalisée par les équipes achats en fonction de la criticité des données échangées et des accès IT

accordés. Un retour terrain : lors d'un accompagnement d'une PME de fabrication de pièces aéronautiques en 2025, la reclassification comme fournisseur "Critical" suite à l'intégration dans le portail collaboratif Airbus a déclenché une obligation de mise à niveau AirCyber dans les 6 mois — une contrainte non anticipée par la direction, qui a nécessité un investissement sécurité d'environ 80 000 euros.

Safran Cybersecurity : programme SCAP pour la supply chain

Safran a développé son propre programme de cybersécurité fournisseurs — le **SCAP (Safran Cybersecurity Assurance Program)** — articulé avec AirCyber mais avec des exigences supplémentaires spécifiques à la dimension défense d'une partie de son activité. Le SCAP impose aux fournisseurs de Safran travaillant sur des programmes de défense sensibles des contrôles additionnels liés à la **protection des informations classifiées** et aux règles ITAR (International Traffic in Arms Regulations) pour les programmes avec des composantes américaines. En 2026, Safran intègre progressivement les résultats AirCyber dans son processus de qualification fournisseurs — un fournisseur avec un niveau AirCyber 3 validé sur BoostAerospace bénéficie d'un allègement du questionnaire SCAP. Les fournisseurs Safran ont accès à des formations cybersécurité cofinancées dans le cadre de l'accompagnement de la supply chain, notamment via des diagnostics CyberDiag ANSSI subventionnés. L'articulation SCAP/AirCyber illustre la tendance de fond dans la filière : convergence progressive vers AirCyber comme baseline commune, avec des couches supplémentaires sectorielles (défense, spatial) selon les spécificités du programme concerné.

DO-326A : la cybersécurité des systèmes aéronautiques embarqués

La norme **DO-326A** (Airworthiness Security Process Specification, publiée par RTCA/EUROCAE) traite d'un périmètre fondamentalement différent d'AirCyber : elle concerne la cybersécurité des *systèmes aéronautiques embarqués* (avionique, systèmes de vol, systèmes de

navigation) dans le cadre du processus de certification de navigabilité. AirCyber s'applique aux systèmes IT des entreprises fournisseurs (laptops, serveurs, réseaux d'entreprise) ; DO-326A s'applique aux systèmes embarqués dans les avions qui font l'objet d'une certification EASA (Agence Européenne de la Sécurité Aérienne). La DO-326A est une norme de cycle de vie du développement sécurisé : elle impose une analyse des menaces de sécurité (Security Threat Analysis) lors de la conception des systèmes, la mise en place de contre-mesures appropriées, et la documentation de la sécurité dans le dossier de certification. En 2026, DO-326A est exigée par l'EASA pour la certification de tous les nouveaux systèmes avioniques et pour les modifications significatives des systèmes existants. La formation des ingénieurs avionique aux exigences DO-326A est un enjeu RH important pour les équipementiers aéronautiques (Safran, Thales, Collins Aerospace) et leurs sous-traitants en développement logiciel embarqué.

Articulation AirCyber et NIS 2 pour les entreprises aéronautiques

Les entreprises aéronautiques françaises soumises à NIS 2 — en tant qu'Entités Essentielles ou Importantes dans les secteurs Transport (aérien) ou Défense — font face à une **double conformité** AirCyber + NIS 2, dont l'articulation est importante à comprendre. Bonne nouvelle : les deux référentiels sont largement alignés dans leurs exigences techniques. La gestion des risques (NIS 2 article 21) correspond aux domaines Gouvernance et Protection d'AirCyber. La sécurité de la chaîne d'approvisionnement (NIS 2 article 21.2.d) correspond directement au domaine Cyber Supply Chain d'AirCyber. La notification d'incidents (NIS 2 article 23) est complémentaire au reporting d'incidents AirCyber exigé par les donneurs d'ordres. La principale différence est le périmètre légal : NIS 2 impose des obligations légales sanctionnables (jusqu'à 10 M€ ou 2% du CA mondial), tandis qu'AirCyber impose des obligations contractuelles (perte de contrats avec les donneurs d'ordres). En pratique, une entreprise aéronautique bien structurée peut construire un programme de conformité unique répondant simultanément aux deux référentiels, avec une économie d'échelle significative par rapport à deux programmes séparés.

CyberDiag ANSSI : outil de diagnostic préalable à AirCyber

Pour les PME aéronautiques en début de démarche AirCyber, le **CyberDiag** de l'ANSSI est un outil de pré-diagnostic accessible et peu coûteux. Ce questionnaire d'auto-évaluation en ligne (environ 30 minutes) évalue le niveau de maturité cyber d'une PME sur 4 niveaux, en s'appuyant sur le guide d'hygiène informatique de l'ANSSI (42 règles). Le CyberDiag est souvent réalisé avant l'auto-évaluation AirCyber proprement dite pour identifier les lacunes les plus importantes et les corriger avant de s'engager dans le processus AirCyber officiel. Des prestataires spécialisés proposent des accompagnements CyberDiag subventionnés — via des dispositifs régionaux (BPI France, Régions) ou sectoriels (GIFAS, Alliance Industrie du Futur) — rendant le coût de la démarche accessible aux plus petites PME. En France, plusieurs dizaines de prestataires sont labellisés ExpertCyber par l'ANSSI, habilités à conduire ces diagnostics dans le cadre du programme national Cybermalveillance. L'accompagnement CyberDiag → AirCyber → certification ISO 27001 constitue une progression logique et progressive pour les PME aéronautiques qui souhaitent construire une maturité cyber durable sans se retrouver submergées par des exigences trop ambitieuses d'emblée.

Coûts de mise en conformité AirCyber pour une PME

La mise en conformité AirCyber pour une PME aéronautique représente un investissement significatif mais réaliste. Les coûts se répartissent en plusieurs postes. La **phase de diagnostic et gap analysis** : réalisée par un prestataire spécialisé, elle coûte entre 5 000 et 15 000 euros selon la taille de l'entreprise et l'étendue du périmètre, et identifie les écarts entre la situation actuelle et le niveau AirCyber cible. Les **investissements techniques** : selon le niveau de départ, ils peuvent inclure le déploiement d'un EDR (5 000-20 000 €), la mise en place de sauvegardes isolées testées (3 000-10 000 €), le renforcement de l'authentification (MFA, PAM — 5 000-15 000 €), et le renforcement des pare-feux et de la segmentation réseau (5 000-20 000 €). Les **investissements organisationnels** : rédaction des politiques de sécurité, formation des équipes, désignation et formation d'un référent sécurité (5 000-15 000 €). Les **frais de plateforme BoostAerospace** : adhésion annuelle (2 000-5 000 €). Au total, la mise à niveau d'une PME de

50 salariés de niveau 1 vers le niveau 3 coûte typiquement entre 30 000 et 80 000 euros sur 12 à 18 mois. Des financements existent : Bpifrance (prêt numérique, subventions régionales), crédit d'impôt innovation pour les dépenses de cybersécurité liées aux projets R&D, et cofinancements du GIFAS ou des donneurs d'ordres dans le cadre de leurs programmes de développement de la supply chain.

Programme national AirCyber : accompagnement et formations

Le programme AirCyber ne se limite pas au questionnaire d'auto-évaluation — il inclut un dispositif d'**accompagnement et de formation** pour les PME de la filière. Des sessions de sensibilisation collectives sont organisées régulièrement par les régions aéronautiques (Occitanie, Ile-de-France, Nouvelle-Aquitaine) avec le soutien des pôles de compétitivité aéronautiques (Aerospace Valley, Hexadrone). Des formations spécifiques AirCyber sont disponibles via des organismes partenaires, certifiés Qualiopi pour la prise en charge OPCO. Un **réseau de prestataires référencés** AirCyber — ayant suivi une formation spécifique au référentiel — est disponible pour accompagner les PME dans leur démarche. Ces prestataires connaissent les exigences des donneurs d'ordres et peuvent rapidement identifier les écarts prioritaires à corriger. Le GIFAS publie régulièrement des guides pratiques et des retours d'expérience de PME ayant réalisé leur montée en maturité AirCyber — des ressources précieuses pour les responsables sécurité et les dirigeants de PME qui s'engagent dans la démarche. L'objectif annoncé par le GIFAS est d'avoir 80% des fournisseurs critiques de niveau 3 ou supérieur d'ici 2027 — un objectif ambitieux qui nécessite une accélération significative de la démarche.

Audits AirCyber réalisés par les donneurs d'ordres

Au-delà de l'auto-évaluation sur BoostAerospace, les donneurs d'ordres aéronautiques se réservent le droit de conduire des **audits de vérification** chez leurs fournisseurs critiques. Ces audits, réalisés par les équipes cybersécurité internes ou par des prestataires PASSI mandatés,

vérifient la conformité réelle par rapport aux déclarations de l'auto-évaluation AirCyber. Un écart significatif entre la déclaration et la réalité peut conduire à une suspension de la qualification fournisseur — une conséquence commerciale majeure. La préparation à ces audits passe par la **documentation rigoureuse** de chaque contrôle déclaré : un anti-virus déclaré déployé sur 100% des postes doit être prouvable par une capture d'écran de la console de management, un rapport d'inventaire, etc. L'implémentation de solutions permettant de **générer automatiquement des preuves** de conformité (dashboards de sécurité, rapports automatisés d'EDR, journaux de sauvegarde) facilite considérablement la préparation aux audits. Une bonne pratique : réaliser soi-même un audit interne AirCyber annuel avec un prestataire externe avant l'auto-évaluation officielle, permettant d'identifier et de corriger les écarts avant de les partager sur BoostAerospace.

AirCyber et protection des données de conception : lien avec le secret des affaires

La cybersécurité dans la supply chain aéronautique est étroitement liée à la **protection des données de conception** (CAO, spécifications techniques, données d'essais) échangées entre donneurs d'ordres et fournisseurs. Ces données constituent des actifs stratégiques — leur vol ou leur compromission peut avoir des conséquences en termes de compétitivité, de propriété intellectuelle et parfois de sécurité nationale. La loi sur le **secret des affaires** (transposition de la directive UE 2016/943 en droit français) impose aux entreprises de mettre en place des mesures de protection raisonnables pour les informations qu'elles souhaitent protéger — ce qui inclut des mesures techniques et organisationnelles de cybersécurité. AirCyber répond directement à cette exigence légale en définissant un niveau minimum de protection pour les entreprises de la supply chain. Les **DRM (Digital Rights Management)** et les plateformes d'échange sécurisé utilisées dans la filière (comme BoostAerospace lui-même, ou des solutions de transfert de fichiers sécurisé comme SFTP avec authentification mutuelle) doivent être conformes aux niveaux de protection requis. La classification des données de conception selon leur sensibilité (publique, confidentielle, très confidentielle, Export Control) et l'application de contrôles de sécurité

adaptés à chaque niveau est une pratique recommandée par AirCyber et exigée par les contrats des donneurs d'ordres.

Évolutions prévues d'AirCyber : vers une certification tierce ?

Le programme AirCyber est actuellement basé sur l'auto-évaluation déclarative, avec des audits ponctuels par les donneurs d'ordres. Une évolution vers un système de **certification par des tiers indépendants** est en discussion au sein du GIFAS, s'inspirant du modèle CMMC américain (Cybersecurity Maturity Model Certification) qui impose une certification par des organismes accrédités (C3PAO) pour les niveaux de maturité les plus élevés. Cette évolution permettrait une plus grande confiance dans les niveaux déclarés mais augmenterait significativement les coûts et la complexité pour les PME. Une approche intermédiaire — certification optionnelle pour les fournisseurs souhaitant attester d'un niveau AirCyber élevé auprès de plusieurs donneurs d'ordres simultanément — est également en discussion. L'articulation avec les certifications existantes (ISO 27001, HDS pour la santé) est un sujet de travail actif : une reconnaissance mutuelle partielle éviterait la multiplication des audits pour les entreprises déjà certifiées. En 2026, AirCyber reste une démarche déclarative mais la trajectoire vers une certification tierce semble inéluctable, particulièrement pour les fournisseurs des programmes de défense et de spatial les plus sensibles.

AirCyber pour les ETI et grandes entreprises de la supply chain

Si AirCyber est souvent présenté comme un programme pour les PME, les **ETI et grandes entreprises** de la supply chain aéronautique (équipementiers de rang 1 et 2 avec plusieurs milliers de salariés) ont leurs propres défis de conformité. Pour ces entreprises, l'enjeu n'est pas la mise en place des contrôles de base (déjà généralement en place) mais leur **documentation et leur pilotage** selon la logique AirCyber, et leur extension à l'ensemble des filiales et sites géographiques. La gestion des accès privilégiés (PAM) sur des environnements IT complexes, la

surveillance des réseaux de production (OT/IT convergence), et la gestion de la cybersécurité dans les projets de développement de nouveaux systèmes sont les domaines où les ETI doivent généralement progresser pour atteindre le niveau 4 ou 5 AirCyber. Pour ces entreprises, l'alignement AirCyber avec les certifications ISO 27001 existantes (ou en cours) est la voie la plus efficace — la documentation ISO 27001 répond à la majorité des exigences AirCyber et la certification tierce renforce la crédibilité de l'auto-évaluation auprès des donneurs d'ordres.

Financement de la mise en conformité AirCyber : aides disponibles en France

Plusieurs dispositifs de **financement public** permettent aux PME aéronautiques de couvrir tout ou partie des coûts de leur mise en conformité AirCyber. Le **Prêt Numérique Bpifrance** (jusqu'à 100 000 € sans garantie pour les PME) est accessible aux entreprises investissant dans leur transformation numérique incluant la cybersécurité. Les **subventions régionales** via les DREETS et les Régions (notamment Occitanie et Nouvelle-Aquitaine, fortement impliquées dans l'aéronautique) couvrent parfois jusqu'à 50% des investissements en diagnostic et conseil cybersécurité pour les PME industrielles. Le dispositif **CyberDiag ANSSI subventionné**, déployé par le réseau Cybermalveillance via des prestataires ExpertCyber labellisés, permet des diagnostics à coût réduit (moins de 1 500 € pour une PME de moins de 50 salariés). Les **OPCO** (Opérateurs de Compétences) prennent en charge les formations cybersécurité certifiées Qualiopi pour les salariés des PME, incluant les formations AirCyber spécifiques. Le **crédit d'impôt innovation** (CII, 30% des dépenses éligibles pour les ETI) peut s'appliquer aux projets de développement de nouvelles capacités de sécurité informatique. Enfin, des programmes spécifiques de la filière aéronautique — notamment les actions collectives UIMM et les programmes de développement fournisseurs d'Airbus et Safran — incluent parfois des volets cybersécurité avec cofinancements directs. La mobilisation de ces différentes sources de financement peut couvrir 40 à 60% du coût total d'une mise en conformité AirCyber pour une PME éligible.

Chiffrement des données échangées dans la supply chain : bonnes pratiques

L'échange de données techniques sensibles entre donneurs d'ordres et fournisseurs dans la supply chain aéronautique nécessite des mécanismes de **chiffrement robustes** à chaque étape du cycle de vie des données. Pour les données **en transit**, le chiffrement TLS 1.3 doit être appliqué à tous les échanges via portails web, API ou transferts de fichiers. Les protocoles de transfert non chiffrés (FTP, HTTP) sont prohibés. Pour les données **au repos** sur les systèmes des fournisseurs, le chiffrement des disques (BitLocker, VeraCrypt) et des bases de données (TDE) est exigé pour les données de conception classifiées. Pour les données **en cours d'utilisation**, des solutions de DRM (Digital Rights Management) permettent de contrôler l'utilisation des fichiers même une fois téléchargés chez le fournisseur — une couche de protection supplémentaire particulièrement utile pour les données Export Control. Les **emails chiffrés** (S/MIME ou PGP) sont recommandés pour l'échange de données sensibles hors des portails sécurisés — en pratique, peu utilisés en raison de la complexité de gestion des certificats, au profit des portails sécurisés. Les exigences de chiffrement d'AirCyber s'alignent sur celles du référentiel de sécurité des systèmes d'information de l'ANSSI et sur le guide Cyber des données soumises à ITAR/EAR (Export Administration Regulations américaines), applicable aux programmes de coopération franco-américains. La gestion rigoureuse des clés de chiffrement — stockage sécurisé, rotation régulière, procédure de révocation — est un prérequis souvent négligé que les audits AirCyber révèlent fréquemment comme lacunaire.

Perspectives : AirCyber 2.0 et l'intégration de l'IA dans la conformité

Le programme AirCyber est en évolution constante pour s'adapter aux nouvelles menaces et aux nouvelles technologies. Plusieurs évolutions sont anticipées pour la version 2.0 en cours de discussion au sein du GIFAS. Premièrement, l'intégration d'exigences spécifiques aux **systèmes IA utilisés dans la conception ou la production aéronautique** — suite à l'AI Act, les fournisseurs utilisant des outils IA dans leurs processus devront documenter leurs pratiques conformément aux obligations GPAI. Deuxièmement, le renforcement des exigences sur la **sécurité des environnements cloud** : de nombreux fournisseurs migrent leurs PLM et ERP vers

le cloud, avec des configurations de sécurité cloud spécifiques à documenter. Troisièmement, l'intégration de la **chaîne logistique logicielle** (Software Bill of Materials, SBOM) pour les fournisseurs développant des logiciels embarqués aéronautiques. Quatrièmement, des mécanismes de **certification continue** basés sur des outils de monitoring automatique de la posture cyber, remplaçant progressivement les auto-évaluations ponctuelles. Ces évolutions maintiendront AirCyber en phase avec les meilleures pratiques internationales et renforceront sa crédibilité comme référentiel sectoriel de référence pour la supply chain aéronautique française.

Comparaison AirCyber, TISAX et CMMC : les référentiels sectoriels en Europe

AirCyber s'inscrit dans un mouvement plus large de **référentiels de maturité cybersécurité sectoriels** qui émergent dans différentes industries en Europe et en Amérique du Nord. **TISAX (Trusted Information Security Assessment Exchange)**, développé par l'ENX Association pour l'industrie automobile, est le modèle le plus mature en Europe : il inclut une évaluation par des auditeurs tiers accrédités et un mécanisme de partage des résultats entre membres (constructeurs automobiles et fournisseurs). TISAX est désormais exigé par BMW, Mercedes, Volkswagen et leurs fournisseurs en Europe, et son modèle d'audit tiers accrédité est considéré par le GIFAS comme une évolution naturelle pour AirCyber. Le **CMMC (Cybersecurity Maturity Model Certification)** américain, imposé par le Département de la Défense américain à ses fournisseurs, est plus contraignant avec une certification obligatoire par des C3PAO (Certified Third-Party Assessment Organizations) accrédités pour les niveaux 2 et 3. Les fournisseurs aéronautiques français travaillant sur des programmes avec une composante américaine (F-35, programmes de coopération OTAN) doivent se conformer au CMMC en plus d'AirCyber — une double charge que l'alignement progressif entre les deux référentiels devrait alléger. La convergence internationale de ces référentiels sectoriels vers des standards communs (basés sur NIST CSF, ISO 27001 et IEC 62443) est la tendance de fond qui devrait simplifier la conformité multi-référentielle pour les entreprises aéronautiques mondiales d'ici 2028-2030.

Sécurité des outils de CAO collaborative : Catia, NX et leurs extensions

Les outils de **CAO (Conception Assistée par Ordinateur)** collaboratifs utilisés dans la supply chain aéronautique — CATIA V5/V6 (Dassault Systèmes), Siemens NX, PTC Creo — sont au cœur des échanges de données de conception sensibles. Leur sécurisation est un enjeu spécifique à AirCyber. Ces outils fonctionnent souvent sur des postes Windows dédiés avec des licences flottantes sur des serveurs réseau, créant une surface d'attaque spécifique : le serveur de licences et les bases de données CAO sont des cibles d'exfiltration de données de premier ordre. Les fichiers CAO eux-mêmes (formats CATPART, CATDRAWING, JT, Parasolid) contiennent souvent des données Export Control ou ITAR non marquées comme telles dans les métadonnées, ce qui complique leur protection. Les mesures de sécurité spécifiques incluent : chiffrement des bases de données CAO au repos (TDE pour SQL Server ou Oracle), contrôle d'accès basé sur les rôles dans les PDM/PLM (ENOVIA, Windchill, Teamcenter) avec journalisation des accès aux fichiers sensibles, protection DRM des fichiers CAO partagés avec des partenaires externes (solutions de DRM CAO comme LockLizard ou Microsoft AIP), et monitoring des téléchargements massifs de fichiers CAO depuis les systèmes PLM. Le vol de propriété intellectuelle via des outils CAO mal protégés est l'une des formes d'espionnage industriel les plus préjudiciables pour la filière aéronautique française.

Retour d'expérience : PME aéronautique de 120 salariés — montée AirCyber niveau 3

Pour illustrer concrètement la démarche AirCyber, voici un retour d'expérience d'une PME de sous-traitance aéronautique de 120 salariés (usinage de précision, fournisseur rang 2 d'Airbus et Safran) que nous avons accompagnée en 2025. Situation de départ : niveau AirCyber estimé 1,5, pas de politique de sécurité formalisée, antivirus basique sur les postes, pas de MFA, sauvegardes sur NAS local non testé, un seul informaticien polyvalent. Objectif : atteindre le niveau 3 AirCyber en 12 mois pour maintenir la qualification fournisseur Airbus. Les **premières actions immédiates** (mois 1-3, budget ~15 000 €) : déploiement MFA sur Office 365 et VPN, activation

du Microsoft Defender for Business (EDR inclus dans Microsoft 365 Business Premium), mise en place de sauvegardes cloud chiffrées avec tests de restauration mensuels automatisés, et rédaction d'une politique de sécurité simple (5 pages) couvrant les bases. Les **actions intermédiaires** (mois 4-9, budget ~30 000 €) : segmentation réseau (VLAN production/bureau), déploiement d'un pare-feu de nouvelle génération, formation anti-phishing des 120 collaborateurs, désignation d'un référent sécurité (ingénieur qualité formé), et rédaction des procédures de gestion des incidents et de continuité d'activité. À 12 mois, l'auto-évaluation AirCyber a été réalisée sur BoostAerospace avec un score de niveau 3,2 — objectif atteint. Coût total de la démarche : environ 55 000 euros sur 12 mois, financement partiel via un prêt Bpifrance Numérique. L'investissement a été rentabilisé en moins de 6 mois via le maintien des contrats Airbus et l'obtention d'un nouveau contrat Safran dont l'une des conditions était un niveau AirCyber 3 minimum.

AirCyber et sous-traitance offshore : défis spécifiques

La supply chain aéronautique est mondiale — de nombreux fournisseurs français ont eux-mêmes des sous-traitants en Asie, en Europe de l'Est ou en Amérique du Sud. Cette **sous-traitance offshore** crée des défis spécifiques pour la conformité AirCyber. Le domaine Cyber Supply Chain du questionnaire AirCyber évalue précisément comment l'entreprise gère la cybersécurité de ses propres fournisseurs — y compris les fournisseurs offshore. Les exigences incluent : contrats incluant des clauses de sécurité (politique de mots de passe, restriction d'accès aux données, notification d'incidents), évaluation de la maturité sécurité des fournisseurs critiques, et droits d'audit. En pratique, imposer et vérifier des niveaux de sécurité à des fournisseurs en Chine, en Inde ou en Tunisie est un défi opérationnel significatif. Des solutions pragmatiques incluent : la classification des données partagées avec chaque fournisseur offshore (éviter de partager des données ITAR ou classifiées avec des fournisseurs dans des pays à risque), l'utilisation de portails d'échange sécurisé contrôlés côté France (les fournisseurs offshore accèdent uniquement au portail, pas aux systèmes internes), et des clauses contractuelles de droit d'audit exercées par des tiers locaux dans le pays du fournisseur. La vérification de la conformité

offshore reste un défi que le questionnaire AirCyber adresse mais que peu d'entreprises ont entièrement résolu.

Gestion des accès aux systèmes d'information des donneurs d'ordres

Un enjeu majeur de cybersécurité dans la supply chain aéronautique est la gestion des **accès des fournisseurs aux systèmes d'information des donneurs d'ordres**. De nombreux fournisseurs accèdent directement aux portails de commande, aux systèmes de CAO collaboratifs, aux applications MES (Manufacturing Execution Systems) ou aux portails qualité d'Airbus, Safran ou Dassault. Ces accès, s'ils sont compromis côté fournisseur, peuvent permettre à un attaquant d'entrer directement dans les systèmes du donneur d'ordres. C'est pourquoi les donneurs d'ordres imposent des exigences croissantes sur les conditions d'accès à leurs systèmes : **MFA obligatoire** pour tous les accès portail, sessions enregistrées et auditées, politique de gestion des comptes fournisseurs (durée de validité, révocation automatique à la fin du contrat), et vérification régulière que les comptes actifs correspondent à des personnes en activité chez le fournisseur. AirCyber intègre ces exigences dans son domaine Protection (gestion des accès) et dans son domaine Supply Chain (sécurité des accès tiers). Un fournisseur qui ne respecte pas les conditions d'accès imposées par son donneur d'ordres risque la suspension de ses accès — avec des conséquences opérationnelles directes sur sa capacité à livrer.

Sensibilisation des dirigeants de PME aéronautiques

L'un des obstacles majeurs à la mise en conformité AirCyber dans les PME aéronautiques est le manque de **sensibilisation des dirigeants** aux enjeux cybersécurité. Pour un chef d'entreprise de PME industrielle focalisé sur la production, les carnets de commandes et les marges, la cybersécurité est souvent perçue comme une contrainte administrative supplémentaire imposée par les grands groupes. Le programme AirCyber et l'IHEDN ont développé des formats de sensibilisation adaptés aux dirigeants : des conférences courtes (2 heures) présentant des cas

concrets d'incidents cyber dans la supply chain aéronautique, des simulations d'attaque en "table-top exercise" illustrant l'impact opérationnel d'un ransomware sur une PME industrielle, et des témoignages de dirigeants de PME ayant subi des incidents cyber documentant l'impact financier réel. L'argument le plus efficace auprès des dirigeants n'est pas réglementaire mais commercial : **la non-conformité AirCyber peut conduire à la perte de marchés** avec Airbus, Safran ou Dassault — un argument auquel les dirigeants de la supply chain aéronautique sont particulièrement sensibles dans un contexte de montée en cadence des programmes A320neo et A350.

Threat intelligence aéronautique : menaces spécifiques à la filière

La filière aéronautique est une cible privilégiée des groupes APT (Advanced Persistent Threats) étatiques en raison de la valeur stratégique de ses données : plans de conception d'aéronefs militaires, technologies propriétaires, données de supply chain permettant de cartographier les capacités industrielles. Les groupes APT connus pour cibler spécifiquement l'aéronautique incluent **APT10** (Chine, ciblant la supply chain technologique mondiale), **APT41** (Chine, espionnage industriel), **Fancy Bear/APT28** (Russie, intérêts géopolitiques liés à la défense) et **Lazarus Group** (Corée du Nord, vol de technologies et de fonds). En France, l'ANSSI documente régulièrement des intrusions dans des entreprises industrielles françaises, dont certaines dans la filière aéronautique et défense. La spécificité de ces attaques : elles sont longues, patientes et silencieuses — l'objectif est l'exfiltration de données sur des mois ou des années sans perturbation des opérations. La détection de ces attaques nécessite un monitoring comportemental avancé que la plupart des PME ne mettent pas en place. Les **Indicators of Compromise (IOC)** spécifiques aux APT ciblant l'aéronautique sont disponibles via les flux MISP de l'ANSSI, auxquels les OIV et OSE du secteur ont accès. Pour les PME non OSE, l'adhésion à des groupes de partage de renseignement sectoriel (ISAC Aéronautique, si créé) permettrait d'accéder à une threat intelligence adaptée à leur contexte.

Coordination entre RSSI et responsable qualité dans la supply chain aéronautique

Dans les entreprises aéronautiques, le **responsable qualité** joue un rôle central dans la gestion de la relation avec les donneurs d'ordres — il est souvent l'interlocuteur principal pour les audits clients et la gestion des exigences contractuelles. La cybersécurité AirCyber doit donc être portée conjointement par le responsable qualité et le RSSI (ou le référent sécurité dans les PME sans RSSI dédié). Cette collaboration est indispensable pour plusieurs raisons : le questionnaire AirCyber est souvent reçu et traité en premier par le service qualité, qui doit le transmettre au référent sécurité avec le contexte approprié ; les audits AirCyber des donneurs d'ordres sont généralement conduits avec la participation du service qualité ; et la mise en conformité AirCyber impacte des processus qualité existants (gestion documentaire, contrôles de processus) qu'il faut aligner avec les nouvelles exigences sécurité. Dans les PME, la création d'un **binôme Qualité-Sécurité** dédié à la conformité AirCyber, avec un mandat clair de la direction générale, est la structure organisationnelle la plus efficace observée dans les PME qui ont réussi leur montée en maturité AirCyber dans des délais raisonnables.

FAQ — AirCyber et BoostAerospace 2026

AirCyber est-il obligatoire pour tous les fournisseurs aéronautiques ?

AirCyber n'est pas imposé par la loi mais par les contrats des donneurs d'ordres. En 2026, Airbus, Safran, Dassault et Thales imposent contractuellement à leurs fournisseurs critiques de réaliser l'auto-évaluation AirCyber et de la partager via BoostAerospace. Pour les fournisseurs considérés comme "Standard" (accès aux données non sensibles), l'exigence est généralement moins stricte — sensibilisation recommandée mais pas d'obligation formelle. La tendance est à une extension progressive des exigences à l'ensemble de la supply chain, quel que soit le rang de sous-traitance.

Quelle est la différence entre AirCyber et ISO 27001 ?

AirCyber est un référentiel sectoriel de maturité cyber spécifique à l'industrie aéronautique française, basé sur une auto-évaluation. ISO 27001 est une norme internationale de management de la sécurité de l'information, avec certification tierce. Les deux sont complémentaires : ISO 27001 apporte une rigueur processuelle et une reconnaissance internationale ; AirCyber apporte un langage commun dans la supply chain aéronautique française. Une entreprise certifiée ISO 27001 peut généralement démontrer un niveau AirCyber 4 ou 5 sans effort supplémentaire majeur, sous réserve de compléter les sections spécifiques au contexte aéronautique.

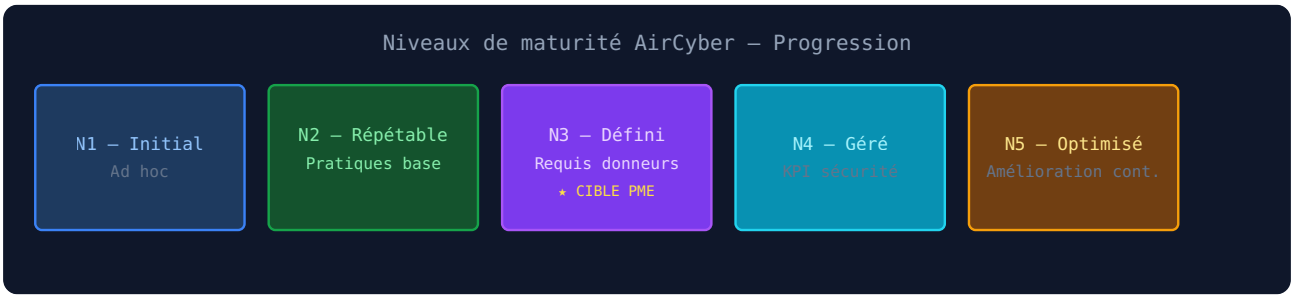
BoostAerospace est-il accessible aux fournisseurs non-français ?

Oui, BoostAerospace est ouvert aux fournisseurs internationaux d'Airbus, Safran et des autres membres fondateurs. La plateforme est disponible en anglais et en français. Des équivalences avec des référentiels locaux (CMMC pour les fournisseurs américains, TISAX pour les fournisseurs automobiles allemands travaillant aussi pour l'aéro) sont en cours de discussion mais non encore formalisées. Les fournisseurs non-européens peuvent réaliser l'auto-évaluation AirCyber et la partager via BoostAerospace comme tout autre fournisseur.

Combien de temps prend la mise en conformité AirCyber niveau 3 pour une PME partant de zéro ?

Pour une PME de 50 à 200 salariés partant d'un niveau 1 (pratiques ad hoc), la montée vers le niveau 3 AirCyber prend typiquement 12 à 18 mois avec un accompagnement professionnel. Les premiers 3 mois sont consacrés au diagnostic et au plan d'action. Les 6 à 12 mois suivants à la mise en œuvre des mesures techniques et organisationnelles prioritaires. Les derniers 3 mois à la documentation, à la formation des équipes et à la finalisation de l'auto-évaluation. Des facteurs accélérateurs : avoir déjà un référent IT compétent en interne, disposer d'un budget sécurité alloué, et bénéficier d'un soutien actif de la direction générale.

Domaine AirCyber	Questions	Contrôles clés niveau 3	Lien ISO 27001
1 — Gouvernance	~8	Politique SMSI, référent sécurité	Clauses 5, 6
2 — Protection	~12	MFA, EDR, chiffrement, pare-feu	Annexe A.9, A.12, A.13
3 — Défense	~10	SIEM/journalisation, alertes	Annexe A.12, A.16
4 — Résilience	~10	Sauvegardes testées, PCA/PRI	Clause 8, Annexe A.17
5 — Supply Chain	~5	Évaluation fournisseurs, contrats	Annexe A.15



Pour approfondir votre démarche de conformité sectorielle, consultez notre guide sur la cyber assurance (qui couvre les critères spécifiques aux fournisseurs aéronautiques), notre analyse du pentest OT/ICS pour les environnements de production aéronautiques, notre article sur les outils SOC open source pour les PME devant structurer leur détection, et notre guide protocoles OT pour les systèmes de production connectés. Les ressources officielles incluent le programme AirCyber sur le site du GIFAS et la plateforme BoostAerospace pour l'inscription et le partage des auto-évaluations.