AirCyber BoostAerospace : Guide Complet Fournisseurs

> AirCyber Bronze, Silver et Gold : ce que la démarche BoostAerospace apporte aux sous-traitants aéronautiques, exigences Airbus/Safran et financement PME.

AirCyber est le dispositif de labellisation cybersécurité conçu par BoostAerospace, le GIE fondé par Airbus, Safran, Thales et Dassault Aviation pour homogénéiser le niveau de sécurité de la supply chain aéronautique française. Organisé en trois niveaux progressifs — Bronze, Silver et Gold — il définit des exigences croissantes alignées sur le référentiel de l'ANSSI et, au niveau supérieur, sur ISO 27001. Depuis 2023, AirCyber Bronze est devenu une condition contractuelle exigée par les donneurs d'ordre de rang 1 pour leurs fournisseurs directs, et cette exigence descend progressivement dans les rangs inférieurs de la chaîne d'approvisionnement. Mais AirCyber ne se résume pas à un tampon commercial : c'est une démarche qui oblige les sous-traitants à formaliser leur gouvernance du système d'information, à cartographier leurs actifs, à se doter d'une politique de sécurité réelle et à prouver que leurs processus de gestion des incidents et de continuité d'activité existent et fonctionnent. Pour une PME aéronautique qui n'a jamais engagé de démarche de sécurité structurée, AirCyber Bronze représente une transformation profonde — et un marchepied crédible vers ISO 27001. Ce guide analyse ce que la démarche apporte concrètement, ce qu'elle exige, comment la financer et comment s'y préparer.

À RETENIR

Ce que vous devez retenir

AirCyber est créé par les 4 majors de l'aéronautique française — ce n'est pas une certification optionnelle

Bronze = 44 mesures ANSSI + audit assesseur accrédité — exigé par Airbus et Safran depuis 2024

La démarche structure réellement le SI : PSSI, gestion des incidents, PCA, inventaire des actifs

Alignement naturel avec ISO 27001 : AirCyber Bronze couvre environ 60 % des contrôles ISO 27001

Les financements France 2030 couvrent jusqu'à 70 % du coût de la démarche

Le label est progressif : commencer par Bronze en 3 à 6 mois est réaliste pour une PME

Qu'est-ce qu'AirCyber BoostAerospace ?

AirCyber est né d'un constat partagé par les quatre majors de l'industrie aéronautique française : la supply chain était le maillon faible de la cybersécurité sectorielle. Airbus, Safran, Thales et Dassault Aviation ont donc constitué le GIE BoostAerospace pour développer un référentiel commun, adapté aux réalités des sous-traitants de toutes tailles — PME de 15 personnes comme ETI de 2 000 salariés. L'objectif n'était pas de créer une certification de plus, mais d'établir un langage commun de la maturité cyber dans la chaîne d'approvisionnement aérospatiale.

La logique est industrielle avant d'être réglementaire : un réseau de fournisseurs est aussi sécurisé que son maillon le plus faible. Une PME sous-traitante de rang 2, qui héberge des plans de conception ou des données de simulation, peut ouvrir une porte d'entrée sur les systèmes critiques d'un grand groupe. AirCyber vise à éliminer ces vulnérabilités systémiques en fixant un socle minimum exigible, vérifiable et progressif.

Le dispositif s'articule en trois niveaux de certification croissante. Chaque niveau fait l'objet d'un audit réalisé par un assesseur accrédité par BoostAerospace, ce qui garantit l'homogénéité et la crédibilité de l'évaluation à travers toute la supply chain. Le label obtenu est valable pour une durée définie, avec des audits de renouvellement pour maintenir le niveau.

Niveau	Périmètre	Nombre de mesures	Durée d'audit	Cible principale
Bronze	Hygiène informatique fondamentale	44 mesures ANSSI	2 jours (assesseur)	PME, TPE, sous-traitants rang 2
Silver	Gestion des risques + tests d'intrusion	Mesures supplémentaires	3 jours	ETI, fournisseurs stratégiques
Gold	SMSI complet, équivalent ISO 27001	Ensemble du référentiel	Audits annuels	Grands groupes, sous-traitants critiques

La question revient souvent : pourquoi ces quatre acteurs ont-ils développé leur propre label plutôt que d'exiger directement ISO 27001 ? La réponse tient en un mot : accessibilité. ISO 27001 représente une démarche de 12 à 24 mois, un investissement de 30 000 à 80 000 euros, et une complexité organisationnelle difficile à absorber pour une PME de 30 personnes. AirCyber Bronze, lui, peut être atteint en 3 à 6 mois, pour un coût ramené à 3 000-5 000 euros après financement public. C'est un standard atteignable qui ne laisse pas de côté la majorité de la supply chain.

Ce que la démarche Bronze apporte concrètement

Au-delà du label, AirCyber Bronze force une transformation opérationnelle réelle. Les 44 mesures ANSSI ne sont pas des cases à cocher : elles imposent de construire — ou de reconstruire — les fondations du système d'information. Voici ce que cette démarche produit concrètement dans une organisation.

> ⚡ **Retour terrain**
>
> Dans mes missions de conformité, j'observe que les entreprises sous-estiment systématiquement le délai de mise en œuvre des mesures techniques. Les mesures organisationnelles (politiques, procédures) s'écrivent en semaines ; les mesures techniques (segmentation réseau, chiffrement, MFA) se déploient en mois. Pour un plan de mise en conformité réaliste, je multiplie toujours les estimations initiales des équipes IT par 2,5 — et je n'ai jamais eu à réduire ce coefficient.

Un inventaire complet du système d'information

La première exigence d'AirCyber Bronze est de savoir ce qu'on a. Cela peut paraître trivial, mais la réalité de nombreuses PME industrielles est différente : des serveurs oubliés sous un bureau, des NAS non patchés depuis trois ans, des comptes utilisateurs de salariés partis depuis deux ans, des applications SaaS souscrites sans validation IT. L'audit ne peut démarrer sans un inventaire documenté et à jour des actifs matériels et logiciels.

Cet inventaire devient ensuite la colonne vertébrale de toute la démarche : il permet d'identifier les systèmes critiques, de prioriser les actions de remédiation et de définir le périmètre sur lequel le label s'applique. Pour beaucoup d'entreprises, c'est la première fois qu'elles disposent d'une vision claire et complète de leur patrimoine informatique.

Une PSSI qui tient la route

AirCyber Bronze exige une Politique de Sécurité des Systèmes d'Information (PSSI) formalisée, validée par la direction et connue de l'ensemble des collaborateurs. Pas un document de 80 pages que personne ne lit : un ensemble cohérent de règles sur la gestion des mots de passe (longueur, renouvellement, MFA), l'usage des appareils personnels (BYOD), les règles d'accès aux systèmes depuis l'extérieur, et la charte utilisateur signée par chaque salarié.

Ce travail de formalisation a une valeur opérationnelle directe : il clarifie les responsabilités, réduit les comportements à risque non malveillants (le technicien qui envoie des plans par Gmail parce que c'est plus simple, le responsable commercial qui utilise son mot de passe sur dix services différents), et crée une base juridique pour traiter les incidents liés à des manquements humains.

La gestion des incidents formalisée

Avant AirCyber, la gestion d'un incident cyber dans une PME industrielle ressemble souvent à ceci : le serveur est tombé, l'IT appelle son prestataire, on tente de comprendre ce qui s'est passé, on reboot, on espère que c'est réglé. AirCyber Bronze exige une procédure documentée : qui est notifié, dans quel délai, avec quel contenu, et par quel canal de communication de secours si la messagerie principale est compromise.

La démarche impose également la tenue d'un registre des incidents de sécurité — même mineurs — et l'obligation de notification à l'ANSSI en cas d'incident significatif. Ce registre a une utilité immédiate : il permet d'identifier les patterns d'incidents récurrents, de mesurer l'évolution dans le temps et de justifier auprès de donneurs d'ordre ou d'assureurs que la sécurité est pilotée de manière structurée.

La continuité d'activité pensée

AirCyber Bronze exige que l'organisation ait réfléchi à sa résilience. Cela passe par un Plan de Continuité d'Activité (PCA) documenté, une Analyse d'Impact sur l'Activité (BIA) identifiant les processus critiques, et des objectifs de reprise définis : RTO (Recovery Time Objective, durée maximale d'interruption tolérable) et RPO (Recovery Point Objective, perte de données

maximale acceptable). Ces définitions semblent techniques, mais leur réalité est simple : si votre ERP tombe un lundi matin, en combien de temps devez-vous le remettre en service, et combien de données pouvez-vous vous permettre de perdre ?

Pour beaucoup de sous-traitants, formuler ces questions pour la première fois est révélateur. La réponse aux deux questions est souvent "immédiatement" et "zéro" — mais les sauvegardes en place ne permettent pas de tenir ces objectifs. AirCyber force à aligner les moyens sur les ambitions.

L'une des questions les plus fréquentes des sous-traitants est : "Si on vise ISO 27001 à terme, est-ce qu'AirCyber Bronze est un passage obligé ou une perte de temps ?" La réponse est sans ambiguïté : AirCyber Bronze est un marchepied, pas une alternative. Concrètement, il couvre environ 60 % des contrôles de l'annexe A d'ISO 27001:2022, avec une focalisation sur les domaines les plus critiques pour l'hygiène informatique. Autrement dit, une organisation labellisée Bronze a déjà accompli plus de la moitié du chemin vers la certification internationale.

Pour une analyse détaillée des convergences et des différences entre les deux référentiels, consultez notre article dédié sur AirCyber vs ISO 27001.

Critère	Bronze	Silver	Gold	ISO 27001
Nombre de mesures	44	~70	~93	93 contrôles (Annexe A)
Type d'audit	Assesseur accrédité	Assesseur + pentest	Audit SMSI complet	Organisme certificateur accrédité COFRAC
Durée d'obtention	3 à 6 mois	6 à 12 mois (depuis Bronze)	12 à 18 mois (depuis Silver)	12 à 24 mois
Coût estimé	5 000 – 15 000 € HT	15 000 – 30 000 € HT	30 000 – 60 000 € HT	30 000 – 80 000 € HT
Reconnaissance	Supply chain aérospatiale FR	Supply chain aérospatiale FR	Niveau proche ISO 27001	Internationale, tous secteurs

La progression Bronze → Silver → Gold n'est pas arbitraire. Silver introduit la gestion des risques formelle, des tests d'intrusion et une analyse approfondie des accès privilégiés. Gold requiert la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI) complet, avec revue de direction périodique, tableaux de bord, et audits internes réguliers — soit exactement ce qu'exige ISO 27001. Un sous-traitant Gold a, dans les faits, la quasi-totalité des briques d'un SMSI ISO 27001 en place. L'ajout de la certification internationale devient alors une formalité de quelques mois supplémentaires.

Ce qu'exigent Airbus, Safran et Thales de leurs fournisseurs

Les exigences des donneurs d'ordre sont la principale motivation pratique des sous-traitants qui s'engagent dans AirCyber. Et ces exigences sont désormais contraignantes, pas seulement incitatives.

Airbus a été le premier à formaliser ses attentes. Depuis 2023, AirCyber Bronze est requis pour l'ensemble des fournisseurs de rang 1 — ceux qui livrent directement à Airbus. La démarche s'étend progressivement aux fournisseurs de rang 2, avec des calendriers qui varient selon les lignes de produits et les périmètres géographiques. Les exigences Airbus pour les fournisseurs incluent également des volets sur la gestion des données ITAR et la protection des informations sensibles de programme.

Safran a rendu AirCyber Bronze obligatoire pour ses fournisseurs stratégiques depuis juin 2024, avec des clauses insérées dans les nouveaux contrats d'approvisionnement. Pour les contrats existants, un délai de mise en conformité a été accordé, mais il s'achève progressivement. Notre guide sur Safran et AirCyber Bronze détaille les clauses contractuelles spécifiques et les procédures de déclaration de conformité.

Thales a adopté une approche par la cartographie des risques : les fournisseurs sont classifiés selon le niveau de sensibilité des données qu'ils traitent, et le niveau AirCyber requis varie en fonction de cette classification. Les sous-traitants qui gèrent des données de défense ou des informations classifiées peuvent se voir imposer Silver, voire Gold.

L'impact concret sur les marchés est réel : des fournisseurs non conformes ont déjà subi des délais dans le renouvellement de contrats, des refus d'extension de périmètre, et dans quelques cas documentés, des déréférencements effectifs. Le label n'est plus une option — c'est une condition d'accès.

Les 3 niveaux de maturité : Bronze, Silver, Gold

Le niveau Bronze est le socle de la démarche. Il s'appuie sur les 44 mesures d'hygiène informatique de l'ANSSI, organisées en cinq familles : gouvernance, authentification, réseaux, mises à jour et sauvegardes. L'audit est réalisé sur site par un assesseur accrédité BoostAerospace, sur une durée de deux jours environ. C'est le niveau exigé par les donneurs d'ordre pour leurs fournisseurs, et c'est le point d'entrée naturel pour toute organisation qui n'a

pas encore engagé de démarche cyber formelle. Pour tout savoir sur l'obtention du Bronze, consultez notre guide pour obtenir la labellisation Bronze.

Le niveau Silver va plus loin : il introduit la gestion formelle des risques (identification, analyse, traitement), impose des tests d'intrusion réguliers sur les périmètres exposés, et renforce les exigences sur la gestion des accès privilégiés et la surveillance des journaux d'événements. Un délai minimum de trois mois est requis entre l'obtention de Bronze et la candidature au Silver, pour permettre à l'organisation de consolider ses pratiques. Découvrez les exigences du niveau Silver pour préparer votre montée en maturité.

Le niveau Gold représente le sommet de la démarche AirCyber. Il exige un SMSI complet avec revue de direction formelle, des audits internes planifiés, une politique de gestion des risques documentée et révisée périodiquement, et des audits de renouvellement annuels. C'est le niveau approprié pour les grands sous-traitants critiques — ceux qui gèrent des informations de programme sensibles, des données à caractère ITAR ou des éléments liés à la défense nationale. La reconnaissance de Gold est quasi équivalente à ISO 27001 dans les appels d'offres aérospatiaux.

Comment financer sa labellisation AirCyber

Le coût brut d'une labellisation AirCyber Bronze — honoraires de l'assesseur et accompagnement à la préparation — se situe généralement entre 5 000 et 15 000 euros HT. Ce montant peut paraître élevé pour une PME industrielle, mais il ne tient pas compte des aides disponibles, qui peuvent couvrir jusqu'à 70 % de la dépense. Pour une analyse complète des dispositifs, consultez notre guide sur le financement PME AirCyber.

France 2030 est le levier principal. Ce plan d'investissement public alloue des fonds spécifiques à la sécurisation des PME industrielles critiques, dont la supply chain aérospatiale est une priorité explicite. Les dépenses éligibles comprennent les honoraires d'assesseur, les prestations de conseil en préparation à l'audit, les outils techniques déployés dans le cadre de la mise en conformité (EDR, gestionnaire de mots de passe, solution de sauvegarde sécurisée), et la formation des équipes.

Les aides régionales complètent le dispositif national. Selon la région d'implantation, les DREETS et les conseils régionaux proposent des aides complémentaires, parfois sous forme d'accompagnement en nature (chèques numérique, accès à des conseillers spécialisés). Les montants et conditions varient significativement d'une région à l'autre.

BPI France propose des prêts spécifiques pour la transformation numérique et cyber des PME, ainsi que des dispositifs de garantie permettant de faciliter l'accès à des financements bancaires complémentaires.

Dispositif	Type d'aide	Taux de prise en charge	Plafond estimé
France 2030 (volet cyber PME)	Subvention directe	Jusqu'à 70 %	Variable selon projet
Aides régionales (DREETS, Conseil Régional)	Subvention ou chèque numérique	20 à 50 %	5 000 – 20 000 €
BPI France (prêt numérique)	Prêt à taux réduit	Financement à 100 %	Variable

En pratique, pour une PME de 50 personnes dont le coût d'accompagnement Bronze atteint 12 000 euros HT, une combinaison France 2030 (70 %) + aide régionale peut ramener le reste à charge à moins de 5 000 euros — soit moins d'un poste de travail. Sur cette base, refuser de s'engager dans la démarche revient à prendre le risque de perdre des marchés dont la valeur est sans commune mesure avec cet investissement.

Comment se préparer à l'audit assesseur

La préparation à l'audit AirCyber Bronze s'organise en trois temps distincts : l'auto-évaluation, la remédiation, et l'audit lui-même. Comptez en moyenne 4 à 6 semaines pour l'auto-évaluation, 2 à 4 mois pour la remédiation selon l'état de départ, et 2 jours d'audit sur site. Pour un inventaire complet des documents à préparer pour l'audit, consultez notre ressource dédiée.

Les 44 mesures ANSSI se répartissent en cinq familles thématiques :

Famille	Exemples de mesures clés	Documents attendus
Gouvernance	PSSI, charte utilisateur, inventaire actifs, formation	PSSI signée, registre actifs, attestation de sensibilisation
Réseaux	Segmentation, filtrage entrant/sortant, Wi-Fi sécurisé	Schéma réseau, règles de pare-feu, inventaire points d'accès
Authentification	MFA sur accès distant et comptes privilégiés, politique MDP	Politique mot de passe, liste comptes à privilèges, preuve MFA
Mises à jour	Gestion des correctifs, EOL, vulnérabilités critiques	Procédure patch, rapport de vulnérabilités, inventaire logiciels
Sauvegardes	Règle 3-2-1, tests de restauration, chiffrement	Plan de sauvegarde, journal de tests de restauration

Le rôle de l'assesseur accrédité est central dans la démarche. Ce n'est pas un auditeur purement vérificateur : il dispose d'une marge d'appréciation sur la maturité des pratiques et peut accompagner l'organisation dans sa préparation, tant qu'il ne se trouve pas en situation de conflit d'intérêts (l'assesseur ne peut pas auditer une organisation qu'il a lui-même accompagnée). Pour savoir comment choisir son assesseur accrédité, référez-vous à notre guide de sélection.

Les entreprises qui réussissent le mieux leur audit Bronze sont celles qui ont engagé une démarche documentaire rigoureuse avant l'arrivée de l'assesseur : toutes les preuves (politiques, registres, journaux, attestations) sont rassemblées dans un dossier structuré, et les équipes techniques ont été briefées sur les éléments à présenter. L'audit ne doit pas être une surprise : c'est une validation d'un état déjà atteint.

Notre centre de ressources AirCyber regroupe l'ensemble des guides, modèles de documents et ressources pratiques pour préparer votre démarche. Et si vous souhaitez être accompagné, découvrez notre accompagnement AirCyber pour les sous-traitants aéronautiques.

NIS 2 et AirCyber : la double conformité supply chain

La directive NIS 2, transposée en droit français, introduit une obligation nouvelle qui change la donne pour les sous-traitants : les entités essentielles et importantes (OIV, OSE, et au-delà) sont désormais responsables de la sécurité de leur chaîne d'approvisionnement. L'article 21 de la

directive impose des mesures sur "la sécurité de la chaîne d'approvisionnement, y compris les relations avec les fournisseurs et les prestataires de services". En clair : si vous êtes sous-traitant d'une entité NIS 2, vos propres pratiques de sécurité deviennent une responsabilité partagée.

AirCyber Bronze répond à une partie significative des exigences que NIS 2 impose indirectement aux fournisseurs des entités régulées. Pour une analyse complète, consultez notre article sur NIS 2 et AirCyber dans la supply chain aérospatiale.

Exigence NIS 2 (Art. 21)	Couverture AirCyber Bronze	Niveau de couverture
Politiques de sécurité SI	PSSI, charte utilisateur, gouvernance	Complète
Gestion des incidents	Procédure incidents, registre, notification ANSSI	Complète
Continuité des activités	PCA, BIA, RTO/RPO	Partielle (Bronze) / Complète (Silver+)
Sécurité de la chaîne d'approvisionnement	Gestion des tiers, clauses contractuelles	Partielle
Mesures de contrôle d'accès et authentification	MFA, politique MDP, comptes privilégiés	Complète

La convergence entre AirCyber et NIS 2 est une opportunité stratégique : les PME sous-traitantes qui obtiennent Bronze disposent d'une base documentaire qui leur permet de répondre aux questionnaires de conformité NIS 2 envoyés par leurs donneurs d'ordre. Deux obligations en une seule démarche, ce qui optimise le retour sur investissement de l'effort de mise en conformité.

FAQ

AirCyber est-il obligatoire pour tous les sous-traitants aéronautiques ?

Non, AirCyber n'est pas une obligation légale universelle — c'est une exigence contractuelle imposée par certains donneurs d'ordre. En pratique, Airbus l'exige pour ses fournisseurs de rang 1 depuis 2023 et Safran depuis juin 2024. Cette obligation se propage progressivement vers les rangs inférieurs de la supply chain via les contrats de sous-traitance. Si votre client direct n'est pas un grand groupe de l'aéronautique, vous n'êtes peut-être pas encore dans le périmètre

d'exigence — mais cela peut changer à tout moment lors d'un renouvellement de contrat. Anticiper est toujours préférable à subir une mise en demeure contractuelle.

Combien de temps faut-il pour obtenir AirCyber Bronze ?

Pour une PME partant de zéro (aucune démarche cyber formalisée), comptez entre 4 et 6 mois en moyenne : 4 à 6 semaines d'auto-évaluation pour établir l'état des lieux, 2 à 4 mois de remédiation pour combler les écarts identifiés, puis l'audit assesseur sur 2 jours. Les organisations qui disposent déjà d'une infrastructure bien administrée et de quelques politiques documentées peuvent réduire ce délai à 2 à 3 mois. En revanche, une entreprise en situation de dette cyber importante (pas de gestion des correctifs, pas de sauvegarde testée, pas de MFA) peut nécessiter 6 à 9 mois. Un accompagnement structuré accélère significativement la démarche.

Quelle est la différence entre AirCyber Bronze et ISO 27001 ?

AirCyber Bronze est un label sectoriel, créé spécifiquement pour la supply chain aérospatiale française, basé sur 44 mesures d'hygiène informatique de l'ANSSI. ISO 27001 est une norme internationale, applicable à tous les secteurs, qui exige la mise en place d'un Système de Management de la Sécurité de l'Information complet avec 93 contrôles dans l'annexe A. En termes de couverture, Bronze correspond à environ 60 % des contrôles ISO 27001. En termes de délai et de coût, Bronze est deux à trois fois moins long et moins coûteux. En termes de reconnaissance, ISO 27001 est reconnu mondialement quand AirCyber l'est principalement dans la supply chain aérospatiale. Les deux sont complémentaires : Bronze structure les fondations, ISO 27001 les consolide et les universalise.

L'assesseur AirCyber peut-il aussi nous préparer à ISO 27001 ?

Oui, à condition qu'il ne s'agisse pas du même assesseur que celui qui réalisera l'audit AirCyber (conflit d'intérêts). De nombreux assesseurs accrédités BoostAerospace sont également consultants ISO 27001. Dans ce cas, ils peuvent intervenir en deux phases distinctes : accompagnement à la préparation AirCyber (hors mission d'audit), puis, une fois le label obtenu, accompagnement complémentaire pour couvrir les 40 % de contrôles ISO 27001 non couverts

par Bronze. C'est le schéma le plus efficace pour les sous-traitants qui visent ISO 27001 à horizon 18-24 mois.

Que se passe-t-il si on échoue à l'audit AirCyber ?

Un échec à l'audit ne signifie pas l'exclusion définitive du dispositif. L'assesseur formule un rapport d'audit détaillé identifiant les écarts, avec leur criticité. L'organisation dispose ensuite d'un délai pour corriger les non-conformités et soumettre à nouveau les preuves. Dans certains cas, un second passage partiel — focalisé sur les points défaillants — est organisé sans refaire l'intégralité de l'audit. Il est important de communiquer proactivement avec son donneur d'ordre en cas de délai : une démarche engagée et un plan de remédiation documenté valent mieux qu'un silence qui peut être interprété comme un désintérêt pour la conformité.

AirCyber s'applique-t-il aux entreprises hors de France ?

AirCyber est un dispositif français, créé par et pour la supply chain aérospatiale française. Cependant, les filiales étrangères de sous-traitants français, et les fournisseurs étrangers d'Airbus France ou de Safran, peuvent également être soumis à l'exigence Bronze via leurs contrats. Dans ce cas, la démarche est techniquement possible — des assesseurs accrédités peuvent intervenir hors de France — mais les aides au financement (France 2030, aides régionales françaises) ne s'appliquent en général qu'aux entités établies en France. Les entreprises étrangères doivent donc assumer l'intégralité du coût.