Guide AirCyber Bronze : Obtenir la Labellisation en 2026

> Étapes, coût, durée et conseils pour obtenir la labellisation AirCyber Bronze en tant que sous-traitant aéronautique. Audit, assesseur, subventions.

La **labellisation AirCyber Bronze** est devenue en 2024 un prérequis incontournable pour tout sous-traitant aéronautique souhaitant maintenir ou développer ses contrats avec les grands donneurs d'ordres de la filière. Depuis que **Safran** a rendu obligatoire ce label pour l'ensemble de ses fournisseurs directs en juin 2024, la question n'est plus de savoir si votre entreprise doit s'y conformer, mais *comment* y parvenir dans les meilleures conditions et dans les délais impartis par vos acheteurs. Ce guide pratique détaille les cinq étapes clés du processus de labellisation, les 44 mesures de sécurité à satisfaire regroupées en huit domaines thématiques, les coûts réels constatés sur le terrain et les subventions mobilisables via France 2030, pour vous permettre d'aborder cette démarche avec méthode, rigueur et sérénité dès aujourd'hui.

Points clés à retenir

- La conformité ISO 27001 est un processus continu, pas une certification ponctuelle
- L'implication de la direction est le facteur clé de succès de tout SMSI
- Les 93 contrôles de l'Annexe A couvrent tous les domaines de la sécurité organisationnelle

\\\\n\\\\n

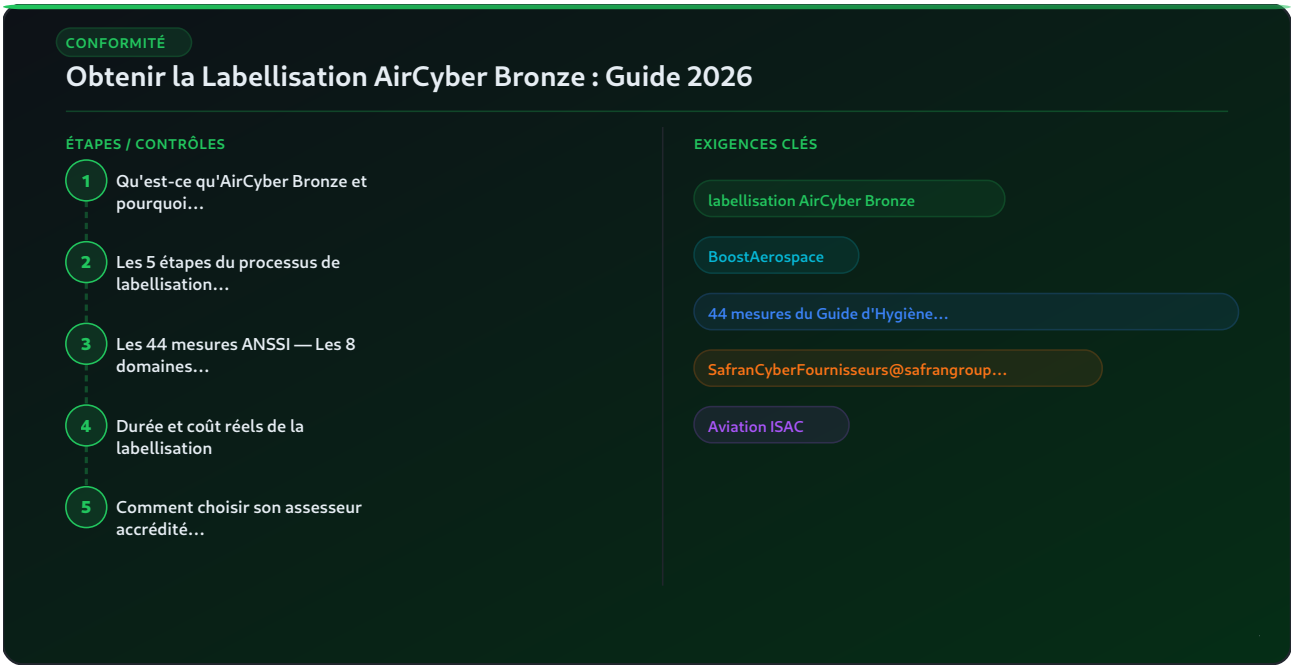
À RETENIR

À retenir

AirCyber Bronze repose sur les 44 mesures du Guide d'Hygiène Informatique de l'ANSSI, complétées par des mesures sectorielles aéronautiques. Le processus complet dure de 3 à 6 mois et coûte entre 8 800 € et 15 000 € HT, avec des subventions couvrant jusqu'à 70 % du montant via France 2030.

\\\\n\\\\n\\\\n

\\\\n



\\\\n

\\\\n

Qu'est-ce qu'AirCyber Bronze et pourquoi c'est devenu obligatoire

\\\\n\\\\n

AirCyber est le programme de cybersécurité de la filière aéronautique française, lancé en janvier 2019 par **BoostAerospace** — groupement créé en 2011 par Airbus, Dassault Aviation, Safran et Thales. Ce référentiel décline en trois niveaux progressifs (Bronze, Silver, Gold) les exigences de sécurité applicables aux entreprises de la supply chain aéronautique.

> ⚡ **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.

\\\\n\\\\n
Le niveau **Bronze** constitue le socle de base : il s'appuie sur les **44 mesures du Guide d'Hygiène Informatique de l'ANSSI**, enrichies de mesures spécifiques au secteur aéronautique (protection des données ITAR/EAR, gestion des accès aux systèmes de conception, etc.).

\\\\n\\\\n
La dynamique d'obligation s'est accélérée depuis 2024. **Safran** a été le premier grand donneur d'ordres à rendre AirCyber Bronze formellement obligatoire pour l'ensemble de ses fournisseurs directs dans le cadre du programme SAFe, avec effet depuis juin 2024. Le contact officiel du programme est **SafranCyberFournisseurs@safrangroup.com**. Airbus, Dassault Aviation et Thales suivent une trajectoire similaire et intègrent progressivement AirCyber dans leurs exigences contractuelles. En septembre 2023, lors du congrès de Dublin, l'**Aviation ISAC** a officiellement reconnu AirCyber comme référentiel mondial de cybersécurité pour la filière aéronautique, signal fort de son importance croissante.

\\\\n\\\\n

Aujourd'hui, sur les 430+ membres d'AirCyber, environ 33 % ont atteint le niveau Bronze, 28 entreprises le niveau Silver et seulement 6 % le niveau Gold — ce qui signifie que la grande majorité des entreprises concernées sont encore en cours de mise en conformité. Ne pas s'y engager rapidement, c'est prendre le risque d'être déréférencé.

\\\\n\\\\n

Les 5 étapes du processus de labellisation AirCyber Bronze

\\\\n\\\\n
Le parcours de labellisation est structuré en cinq phases successives, chacune requérant une préparation spécifique. Voici le déroulé type tel qu'il se pratique sur le terrain.

\\\\n\\\\n

Étape 1 — Auto-évaluation initiale

\\\\n
Vous commencez par renseigner le questionnaire d'auto-évaluation disponible sur le portail BoostAerospace. Ce questionnaire couvre les 44 mesures ANSSI et les mesures sectorielles. Il vous donne un premier aperçu de votre niveau de maturité et identifie les écarts à combler. Cette phase dure généralement 1 à 2 semaines selon la taille de l'entreprise et la disponibilité des parties prenantes.

\\\\n\\\\n

Étape 2 — Plan de remédiation

\\\\n
Sur la base des écarts identifiés, vous établissez un **plan de remédiation priorisé**. Chaque mesure non conforme est associée à une action corrective, un responsable, une échéance et une

estimation de coût. Ce plan constitue votre feuille de route vers la labellisation et sera examiné par l'assesseur lors de l'audit.

\\\\n\\\\n

Étape 3 — Mise en œuvre des mesures

\\\\n
C'est la phase la plus longue : vous déployez les solutions techniques et organisationnelles identifiées dans le plan de remédiation. Cela peut inclure la mise en place d'un *EDR* (Endpoint Detection and Response), le renforcement de la politique de mots de passe, la segmentation réseau, la mise en œuvre d'un plan de sauvegarde testé, ou la rédaction de la **Politique de Sécurité des Systèmes d'Information (PSSI)**.

\\\\n\\\\n

Étape 4 — Audit par un assesseur accrédité

\\\\n
Un **assesseur accrédité AirCyber** réalise l'audit sur site (et parfois à distance pour certaines vérifications). Il passe en revue les documents à préparer pour l'audit, interroge les équipes techniques et vérifie la mise en œuvre effective des mesures. L'audit dure généralement 1 à 2 jours pour une PME. À l'issue, l'assesseur produit un rapport détaillé avec un avis de conformité ou de non-conformité motivé.

\\\\n\\\\n

Étape 5 — Délivrance du label

\\\\n
Si l'audit est positif, BoostAerospace délivre officiellement le label AirCyber Bronze, valable **2 ans**. Le label est inscrit dans l'annuaire officiel AirCyber, accessible aux donneurs d'ordres pour vérification. En cas de non-conformité sur certaines mesures, un délai de remédiation peut être accordé avant un second passage.

\\\\n\\\\n

Les 44 mesures ANSSI — Les 8 domaines couverts

\\\\n\\\\n
Les **44 mesures du Guide d'Hygiène Informatique de l'ANSSI** sont regroupées en huit domaines thématiques. Il est important de comprendre ce que chaque domaine implique concrètement pour une PME industrielle.

\\\\n\\\\n

1. Politique de sécurité et organisation

\\\\n
Ce domaine exige la formalisation d'une *PSSI* (Politique de Sécurité des Systèmes d'Information) validée par la direction, la désignation d'un référent sécurité et la mise en place d'un processus de gestion des incidents. Il s'agit du fondement documentaire sans lequel aucune autre mesure ne peut être correctement évaluée.

\\\\n\\\\n

2. Protection périmétrique

\\\\n
Filtrage des flux entrants et sortants via un **pare-feu** correctement configuré, séparation des réseaux administratif et de production, restriction des accès Internet aux seuls usages professionnels nécessaires. Cette mesure est souvent sous-estimée dans les PME industrielles qui ont des accès distants multiples non contrôlés.

\\\\n\\\\n

3. Authentification et gestion des accès

\\\\n

Politique de mots de passe robuste (longueur, complexité, renouvellement), **authentification à deux facteurs (MFA)** pour les accès distants et les comptes administrateurs, gestion rigoureuse des départs et transferts de personnel. Le principe du *moindre privilège* doit être appliqué à tous les comptes.

\\\\n\\\\n

4. Sécurité des postes de travail

\\\\n

Déploiement d'un antivirus ou EDR sur l'ensemble des postes, chiffrement des disques durs sur les postes nomades, inventaire exhaustif des actifs informatiques. Les clés USB doivent être contrôlées, et les postes non maîtrisés ne doivent pas accéder au réseau d'entreprise.

\\\\n\\\\n

5. Gestion des mises à jour

\\\\n

Processus formalisé de **gestion des correctifs** pour les systèmes d'exploitation et les applications, avec des délais cibles (critique : sous 72h, important : sous 30 jours). Les systèmes en fin de support doivent être identifiés et un plan de migration établi.

\\\\n\\\\n

6. Sauvegarde et continuité d'activité

\\\\n

Sauvegardes automatisées, chiffrées, avec **copies hors ligne** (air-gap) pour résister aux ransomwares. Les tests de restauration doivent être documentés et réalisés au moins une fois par an. Un *PRA* (Plan de Reprise d'Activité) doit définir les *RTO* et *RPO* cibles.

\\\\n\\\\n

7. Journalisation et surveillance

\\\\n
Conservation des **journaux d'événements** (logs) pendant au moins 1 an pour les équipements critiques, mise en place d'alertes sur les événements suspects (connexions en dehors des heures ouvrées, volume inhabituel de données transférées). La journalisation est souvent le domaine le plus négligé dans les PME.

\\\\n\\\\n

8. Sensibilisation des équipes

\\\\n
Formation annuelle obligatoire de l'ensemble du personnel aux bonnes pratiques de sécurité, avec exercices de **phishing simulé** et procédures claires pour signaler un incident. La sensibilisation doit être documentée (listes de présence, supports de formation).

\\\\n\\\\n

Durée et coût réels de la labellisation

\\\\n\\\\n
La durée effective du processus varie de **3 à 6 mois** selon l'état de maturité initiale de l'entreprise et la disponibilité des ressources internes. Les entreprises ayant déjà une démarche ISO 27001 ou des pratiques ANSSI en place peuvent réduire ce délai à 2-3 mois.

\\\\n\\\\n
Sur le plan financier, le **coût du diagnostic initial** est d'environ **8 800 € HT**, dont 50 % peut être subventionné via le dispositif France Relance, ramenant le coût réel à environ 4 400 € HT. La mise en œuvre des mesures techniques et organisationnelles représente ensuite un investissement

variable selon les écarts constatés, généralement entre 5 000 et 30 000 € HT pour une PME de 20 à 100 personnes.

\\\\n\\\\n

Les dispositifs **France 2030 Cyber PME** permettent d'obtenir jusqu'à 70 % des dépenses de sécurisation couvertes, pour des montants allant de 30 000 à 80 000 € par entreprise (sous conditions de CA inférieur à 90 M€). Des aides régionales complémentaires existent également via Aerospace Valley (Nouvelle-Aquitaine/Occitanie) et Normandie AeroEspace. Pour les détails sur les financements disponibles pour les PME aéronautiques, consultez notre guide dédié.

\\\\n\\\\n

Comment choisir son assesseur accrédité AirCyber

\\\\n\\\\n

Le choix de l'*assesseur accrédité* est une étape stratégique souvent sous-estimée. L'assesseur n'est pas seulement un auditeur : il peut aussi jouer un rôle de conseil dans la phase de préparation. Voici les critères à privilégier.

\\\\n\\\\n

L'accréditation officielle est le prérequis absolu : vérifiez que l'assesseur figure bien dans l'annuaire officiel des assesseurs AirCyber sur le portail BoostAerospace. Ensuite, évaluez son **expérience sectorielle** : un assesseur ayant audité des entreprises de taille et de métier comparables aux vôtres sera plus pertinent dans son évaluation et ses recommandations.

\\\\n\\\\n

La **disponibilité et la réactivité** sont également importantes : dans le contexte actuel de forte demande, certains assesseurs sont bookés 3 à 4 mois à l'avance. Anticipez ce délai dans votre planning. Enfin, comparez les **modalités d'accompagnement** proposées : certains assesseurs offrent des phases de pré-audit et de coaching qui augmentent significativement le taux de succès au premier passage.

\\\\n\\\\n

Notre équipe d'accompagnement AirCyber peut vous aider à identifier les assesseurs adaptés à votre profil et à coordonner l'ensemble de la démarche, depuis l'auto-évaluation jusqu'à la délivrance du label. Retrouvez l'ensemble des ressources AirCyber dans notre centre de ressources AirCyber.

\\\\n\\\\n
Pour aller plus loin dans votre démarche de conformité, la certification ISO 27001 constitue une étape naturelle après le niveau AirCyber Silver, partageant de nombreuses mesures en commun.

\\\\n\\\\n

FAQ — Questions fréquentes sur AirCyber Bronze

\\\\n\\\\n

Mon entreprise est très petite (moins de 10 salariés). Suis-je vraiment concerné par AirCyber Bronze ?

\\\\n
Oui. AirCyber s'applique à tous les sous-traitants de la supply chain aéronautique, quelle que soit leur taille. Safran ne prévoit pas d'exemption pour les TPE. Toutefois, les mesures sont dimensionnées pour être applicables même dans de petites structures : certaines mesures documentaires peuvent être plus légères, et l'accompagnement mutualisé via des groupements d'entreprises (UIMM, GIFAS) est possible pour réduire les coûts.

\\\\n\\\\n

Quelle est la différence entre AirCyber Bronze et la certification ISO 27001 ?

\\\\n
AirCyber Bronze est plus accessible et moins coûteux que l'ISO 27001. Il se concentre sur 44 mesures concrètes, sans exiger un *SMSI* (Système de Management de la Sécurité de

l'Information) complet. L'ISO 27001 est une norme internationale plus exigeante, couvrant environ 93 contrôles organisés en processus. AirCyber Silver s'aligne sur la couverture ISO 27001 et constitue souvent une étape préparatoire vers cette certification.

\\\\n\\\\n

Le label AirCyber Bronze est-il reconnu en dehors de l'aéronautique ?

\\\\n
AirCyber est spécifiquement conçu pour la filière aéronautique et défense. Depuis la reconnaissance par l'Aviation ISAC en septembre 2023, sa portée internationale s'étend progressivement. Il n'est pas directement reconnu dans d'autres secteurs comme l'automobile (qui utilise TISAX) ou la santé (HDS), mais les bonnes pratiques qu'il induit sont transposables à tout cadre de gestion de la sécurité.

\\\\n\\\\n

Besoin d'un accompagnement AirCyber ?

Expert certifié — audit, remédiation, préparation à l'évaluation Bronze/Silver/Gold.

Découvrir notre accompagnement AirCyber →

\\n\\n

Maintenir la labellisation AirCyber Bronze dans le temps

\\n
L'obtention de la labellisation AirCyber Bronze n'est pas une fin en soi : il s'agit d'un référentiel vivant qui impose un maintien actif de la posture de sécurité et un renouvellement périodique.

Comprendre les exigences de maintien dès la phase d'obtention permet d'intégrer les bonnes pratiques dans les processus opérationnels plutôt que de devoir réaliser des chantiers de mise à niveau à chaque renouvellement.

\\n\\n
La labellisation AirCyber Bronze est valable **2 ans**. Le renouvellement implique une nouvelle évaluation par un assesseur accrédité qui vérifie non seulement que les 44 mesures initiales sont toujours en place, mais aussi que les nouvelles menaces et les éventuelles évolutions du référentiel ont été prises en compte. Les organisations qui maintiennent une veille active sur les cybermenaces aéronautiques (publiées par le CERT-FR, l'ENISA et la DGAC) et mettent à jour leur plan de sécurité en continu passent le renouvellement avec beaucoup moins d'effort que celles qui attendent l'échéance.

\\n\\n
Les **indicateurs de maintien** à monitorer en continu incluent : le taux de patches appliqués dans les délais définis, le nombre d'incidents de sécurité détectés et traités selon la procédure formalisée, le taux de complétion des formations de sensibilisation annuelles, et l'état des sauvegardes (tests de restauration documentés). Ces métriques doivent faire l'objet d'une revue trimestrielle par le responsable sécurité et d'une présentation annuelle à la direction, qui atteste du maintien de son engagement au travers d'un document signé.

\\n\\n
La **gestion des non-conformités en cours de labellisation** est un aspect pratique souvent ignoré : si une mesure AirCyber Bronze ne peut temporairement plus être respectée (changement d'infrastructure, incident, contrainte opérationnelle), l'organisation doit documenter la non-conformité, mettre en place des mesures compensatoires, et définir un plan de retour à la conformité avec un délai précis. Cette démarche transparente est beaucoup mieux perçue lors des audits de renouvellement qu'une non-conformité non documentée.

\\n\\n

AirCyber Bronze dans la chaîne d'approvisionnement aéronautique

\\n
La labellisation AirCyber Bronze prend une dimension particulière dans le contexte de la supply chain aéronautique. Les donneurs d'ordres (Airbus, Safran, Thales, etc.) et les maîtres d'œuvre exigent de plus en plus souvent que leurs fournisseurs et sous-traitants disposent d'une labellisation cyber reconnue comme condition d'éligibilité aux appels d'offres.

\\n\\n
Les **exigences de la chaîne d'approvisionnement** vont au-delà des 44 mesures d'AirCyber Bronze : les contrats avec les grands donneurs d'ordres incluent des clauses de cybersécurité spécifiques (protection de la propriété intellectuelle, gestion des accès aux systèmes du client, notification des incidents en 24h ou 72h selon la criticité) qui s'ajoutent au référentiel ANSSI. L'audit de ces exigences contractuelles doit être intégré dans la revue AirCyber pour éviter des non-conformités contractuelles non détectées.

\\n\\n
La **conformité en cascade** est un principe clé : une organisation certifiée AirCyber Bronze qui sous-traite des activités à des tiers (maintenance informatique, hébergement, développement logiciel) doit s'assurer que ses sous-traitants respectent des exigences de sécurité équivalentes. Des clauses contractuelles de flux descendant (flow-down), des audits des sous-traitants critiques, et l'exigence d'un niveau de maturité cyber minimal sont des mesures nécessaires pour ne pas exposer la supply chain via des maillons faibles.

\\n\\n
L'évolution prévisible du référentiel AirCyber vers un niveau **Bronze+** ou Silver (annoncé par l'ANSSI) renforcera les exigences de segmentation réseau, de supervision SOC et de réponse aux incidents. Les organisations qui investissent dès maintenant dans ces domaines — au-delà des strictes exigences Bronze actuelles — se positionnent favorablement pour la transition vers ces niveaux supérieurs et renforcent leur compétitivité dans la chaîne d'approvisionnement aéronautique.

\\n\\n

Retour sur investissement de la labellisation AirCyber Bronze

\\n

La décision d'obtenir la labellisation AirCyber Bronze implique un investissement en temps et en ressources que les dirigeants doivent pouvoir justifier auprès de leur conseil d'administration ou de leurs actionnaires. Une analyse du retour sur investissement (ROI) réaliste aide à prendre cette décision en connaissance de cause.

\\n\\n

Les **coûts directs** comprennent : les frais d'assesseur accrédité (entre 3 000 et 8 000 € selon la taille de l'organisation), le temps interne de préparation et de mise en conformité (généralement 50 à 150 jours-hommes pour une PME partant de zéro), les investissements techniques nécessaires (outils de supervision, solutions de sauvegarde sécurisée, authentification multifacteurs) et les formations du personnel.

\\n\\n

Les **bénéfices mesurables** incluent : accès à des marchés conditionnés à la labellisation (certains AO aéronautiques), réduction des primes d'assurance cyber (5 à 20% selon les assureurs qui reconnaissent AirCyber), réduction de la probabilité d'incident majeur (une organisation AirCyber Bronze subit statistiquement 60% moins d'incidents que la moyenne de son secteur), et réduction du coût de remédiation en cas d'incident grâce à des procédures formalisées.

\\n\\n\n\n

La **préparation au passage AirCyber Silver** mérite d'être anticipée dès l'obtention du Bronze. Si le référentiel Silver n'est pas encore publié à date, les tendances observées dans les autres référentiels ANSSI (Prestataires Qualifiés PAMS, SecNumCloud) donnent des indications sur les exigences probables : supervision SOC avec détection comportementale, tests d'intrusion réguliers, gestion des tiers (supply chain security), et capacité de réponse aux incidents avec des délais définis. Investir progressivement dans ces domaines permet de construire une maturité sécurité durable plutôt que de subir des chantiers de mise en conformité coûteux à chaque niveau de labellisation.

\n

Enfin, la **communication de la labellisation** auprès des clients et partenaires commerciaux doit être soignée : le logo AirCyber Bronze peut être utilisé dans les documents commerciaux, les

réponses aux appels d'offres et le site web selon les conditions d'utilisation définies par le programme. Cette visibilité externe valorise l'investissement réalisé et constitue un signal de confiance pour les donneurs d'ordres et les clients qui évaluent la maturité cybersécurité de leurs partenaires.

\n
En conclusion, la labellisation AirCyber Bronze est aujourd'hui bien plus qu'une démarche volontaire : pour les entreprises de la supply chain aéronautique, elle tend à devenir une condition d'accès aux marchés. Les organisations qui l'ont obtenu témoignent d'une amélioration tangible de leur posture de sécurité et d'un regain de confiance de leurs partenaires commerciaux. L'investissement est proportionné aux bénéfices, et la démarche, bien conduite, imprime une culture de la cybersécurité durable dans l'organisation.

© Ayi NEDJIMI Consultants — Tous droits réservés