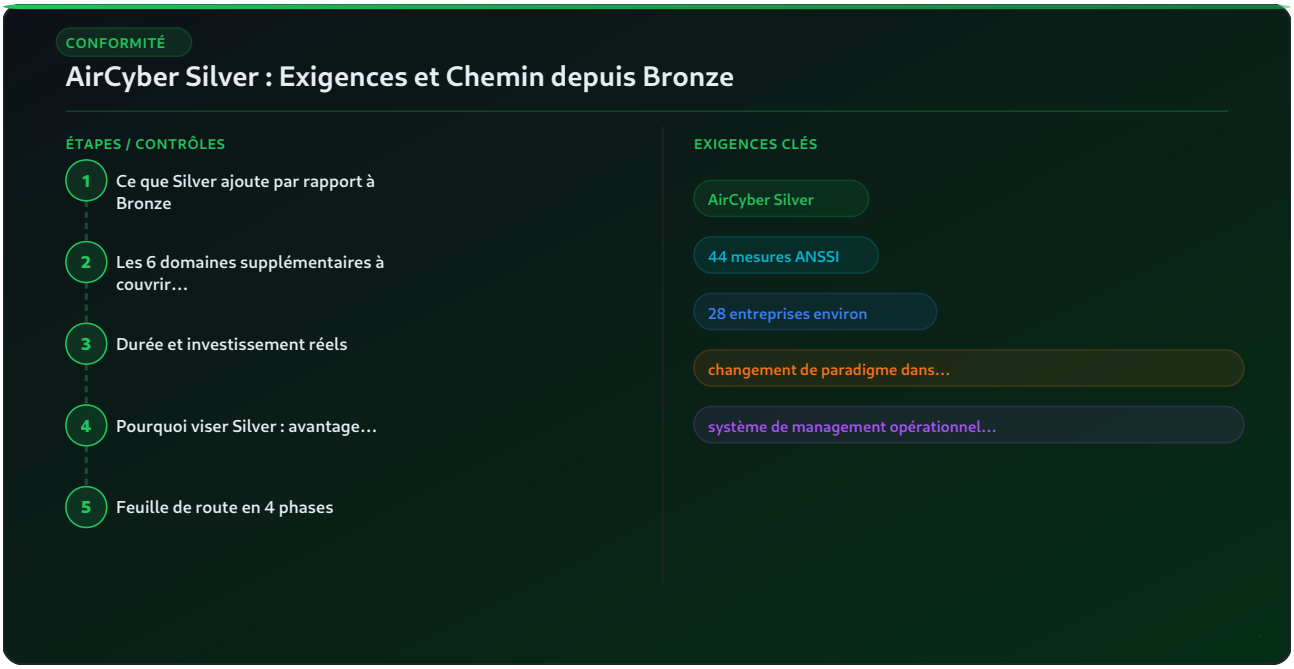
AirCyber Silver : Exigences et Chemin depuis Bronze

> Passer d'AirCyber Bronze à Silver : 6 domaines supplémentaires, coût réel (~100 000 €), 4 phases sur 12 mois. Guide complet pour PME aéronautiques…

Le niveau **AirCyber Silver** représente un saut qualitatif majeur dans la maturité cybersécurité d'une entreprise aéronautique. Si Bronze pose les fondations avec ses **44 mesures ANSSI** et ses exigences sectorielles, Silver exige la construction d'un véritable *Système de Management de la Sécurité de l'Information (SMSI)* aligné sur ISO 27001, avec une couverture des risques systématique et documentée. En 2024, seulement **28 entreprises environ** dans la filière aéronautique et spatiale française ont atteint ce niveau d'excellence — un chiffre qui illustre à la fois la difficulté du parcours et l'avantage concurrentiel distinctif que Silver procure. Cette exclusivité de fait ouvre des portes sur des marchés à forte valeur ajoutée : contrats de défense, projets spatiaux, programmes sensibles nécessitant une maturité cyber démontrée. Si votre entreprise a obtenu Bronze et cherche à capitaliser sur cet investissement pour accéder à ces marchés, ce guide vous fournit la feuille de route concrète pour réussir votre montée en niveau Silver dans les meilleures conditions.



Ce que Silver ajoute par rapport à Bronze

La différence fondamentale entre Bronze et Silver n'est pas seulement quantitative (plus de contrôles), elle est qualitative : Silver exige un **changement de paradigme dans l'approche de la sécurité**. Là où Bronze valide que des mesures techniques et organisationnelles existent, Silver vérifie que l'entreprise dispose d'un **système de management opérationnel et amélioration continue**.

Les apports structurels de Silver par rapport à Bronze :

SMSI formalisé : périmètre défini, politique validée par la direction, processus documentés

Analyse de risques formelle : méthodologie documentée (type ISO 27005 ou EBIOS RM), registre des risques mis à jour

Plan de traitement des risques : priorisé, budgété, suivi par indicateurs

Revue de direction annuelle : procès-verbal, indicateurs de performance sécurité (KPI)

Audit interne : programme d'audit interne planifié et exécuté

Gestion des non-conformités : processus d'identification, d'analyse des causes et de correction

Les 6 domaines supplémentaires à couvrir pour Silver vs Bronze

L'analyse comparative du questionnaire AirCyber identifie **6 domaines prioritaires** qui distinguent Silver de Bronze :

⚡ **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.

1. Gouvernance et organisation de la sécurité : formalisation du RSSI (interne ou externalisé), comité de sécurité avec compte-rendu, budget sécurité tracé, reporting vers la direction générale.

2. Gestion documentaire formalisée : toutes les politiques Bronze deviennent des documents maîtrisés avec versions, approbations, diffusions contrôlées et révisions planifiées selon les guides ANSSI.

3. Gestion des risques structurée : passage d'une approche informelle à une *analyse de risques* méthodologique avec critères de vraisemblance/impact, cartographie des actifs critiques, et traitement formalisé.

4. Continuité d'activité avancée : le PCA simplifié de Bronze devient un plan complet avec tests de reprise (exercices annuels), RTO/RPO définis contractuellement, et procédures de crise documentées.

5. Relations fournisseurs et sous-traitants : extension des exigences de sécurité à votre propre chaîne d'approvisionnement, clauses contractuelles cyber, évaluation des prestataires critiques.

6. Métriques et amélioration continue : tableau de bord sécurité, indicateurs de performance (taux de vulnérabilités corrigées, délai de détection/réponse), revue périodique de l'efficacité des contrôles.

Durée et investissement réels

L'investissement pour atteindre Silver depuis Bronze est significatif. En prenant l'exemple d'une **Entreprise de Mécanique de Structure (EMS) de 80 salariés** avec un SI de taille moyenne :

Conseil et accompagnement RSSI externe : 40 000 – 60 000 €

Outils de sécurité supplémentaires (SIEM léger, EDR complet, scan de vulnérabilités) : 15 000 – 25 000 €/an

Formation et sensibilisation renforcée : 5 000 – 10 000 €

Audit Silver par assesseur accrédité BoostAerospace : 8 000 – 15 000 €

Charge interne mobilisée : 20 – 40 jours/homme sur 12 mois
Total estimé : 70 000 – 110 000 €, soit environ **~100 000 € pour une EMS typique**. La durée réaliste est de **10 à 14 mois** depuis Bronze, en partant d'une base Bronze bien consolidée (minimum 6 mois après Bronze).

Pourquoi viser Silver : avantage concurrentiel et marchés sensibles

L'avantage concurrentiel de Silver est direct et mesurable. Les entreprises certifiées Silver :

Accèdent aux **appels d'offres défense** nécessitant un niveau de maturité cyber élevé

Sont privilégiées sur les **programmes spatiaux sensibles** (CNES, ArianeGroup)

Peuvent sous-traiter à d'autres entités Silver, créant des **écosystèmes de confiance**

Disposent d'un avantage significatif pour obtenir **ISO 27001** avec un effort incrémental minimal

Démontrent une maturité cyber compatible avec les exigences **NIS 2** pour les clients donneurs d'ordre

Feuille de route en 4 phases

Phase 1 — Consolidation Bronze (0-3 mois) : Avant de viser Silver, assurez-vous que votre Bronze est solide. Résolvez les non-conformités mineures de votre dernier audit, formalisez vos politiques de base, et nommez un RSSI (ou engagez un RSSI externalisé avec expertise AirCyber).

Phase 2 — Construction du SMSI (3-7 mois) : Mise en place de la gouvernance formelle, réalisation de l'analyse de risques ISO 27005, rédaction du Plan de Traitement des Risques, définition des KPI sécurité, et mise à jour documentaire en mode maîtrisé.

Phase 3 — Déploiement et test (7-10 mois) : Déploiement des contrôles identifiés dans le PTR, exercice de continuité d'activité, premier audit interne, correction des écarts, et pré-audit Silver avec l'assesseur pour identifier les gaps résiduels.

Phase 4 — Audit Silver et certification (10-14 mois) : Audit officiel par l'assesseur accrédité BoostAerospace, présentation du dossier au Comité de Labellisation, obtention du label Silver et communication auprès de vos clients donneurs d'ordre.

Qui devrait viser Silver ?

Silver n'est pas adapté à toutes les entreprises de la filière. Les critères qui indiquent qu'une entreprise est mûre pour Silver :

Taille : entreprises de plus de **50 salariés** avec un SI structuré

CA : chiffre d'affaires supérieur à **5 M€** avec une part significative en aéronautique

Contrats : accès à des marchés défense, spatiaux ou programmes classificatifs

Ambition : roadmap vers ISO 27001 ou Gold AirCyber dans les 3 ans

Bronze solide : au moins 12 mois de pratique Bronze sans non-conformités majeures

À RETENIR

Points clés à retenir

✓ **Silver ≠ Bronze+** : changement de paradigme vers un SMSI complet

✓ **~28 entreprises** Silver en France = avantage concurrentiel réel

✓ **Budget réaliste** : 70 000 – 110 000 € sur 10-14 mois depuis Bronze

✓ **6 domaines clés** : gouvernance, documents maîtrisés, risques, PCA avancé, fournisseurs, métriques

✓ **Tremplin ISO 27001** : Silver réduit de 70% l'effort pour obtenir ISO 27001

FAQ : AirCyber Silver

Peut-on maintenir Silver sans RSSI interne dédié ?

Oui, à condition de disposer d'un RSSI externalisé avec une mission formalisée et une présence suffisante (généralement 2 à 4 jours par mois minimum). L'assesseur vérifiera que la fonction RSSI est réellement exercée avec des comptes-rendus de réunion, des livrables tracés, et une disponibilité démontrée lors des incidents.

L'audit Silver peut-il être couplé avec l'audit ISO 27001 ?

C'est possible et de plus en plus pratiqué par les assesseurs qui disposent aussi de la qualification pour ISO 27001. Un audit combiné permet de mutualiser la préparation documentaire et de réduire la durée totale de 20 à 30%. Demandez spécifiquement cette option lors de votre sélection d'assesseur.

Que se passe-t-il si l'audit Silver révèle des non-conformités majeures ?

L'assesseur formule des non-conformités majeures et mineures. Pour les majeures, un plan d'action avec délai de correction (généralement 3 à 6 mois) est requis avant que la labellisation soit accordée. Il n'y a pas de "refus" définitif — le processus est itératif et l'accompagnement de l'assesseur peut se poursuivre jusqu'à la conformité.

Articles complémentaires

→ Guide complet : obtenir la labellisation AirCyber Bronze

→ AirCyber vs ISO 27001 : différences et complémentarité

→ Modèles PSSI et politiques de sécurité pour AirCyber Bronze

→ Liste des documents à préparer pour l'audit AirCyber

Prêt à engager le parcours Silver ?

Nos experts AirCyber vous accompagnent de Bronze à Silver avec une feuille de route personnalisée et un accompagnement RSSI externalisé.

Démarrer l'évaluation Silver →

Exigences Techniques AirCyber Silver : Mise en Oeuvre et Preuves

Le niveau AirCyber Silver représente un niveau de maturité cybersécurité significativement plus exigeant que le niveau Bronze, couvrant 39 mesures réparties en 6 domaines selon le référentiel AirCyber de la filière aéronautique française. La transition depuis Bronze vers Silver nécessite généralement 6 à 12 mois de travail de mise en conformité, impliquant des investissements techniques, organisationnels et humains proportionnels à la taille et à la complexité du système d'information de l'entreprise concernée.

Les domaines couverts par le niveau Silver du référentiel AirCyber :

Gouvernance et organisation : politique de sécurité de l'information formalisée et approuvée par la direction, désignation d'un référent cybersécurité avec des responsabilités explicites, plan de formation et de sensibilisation pour tous les employés, et revue annuelle de la politique de sécurité

Protection de l'information : classification des données selon leur sensibilité, chiffrement des données confidentielles en transit et au repos, contrôle des dispositifs amovibles (USB), et politique de bureau propre pour les zones sensibles

Contrôle des accès : gestion des comptes utilisateurs avec principe du moindre privilège, authentification forte (MFA) pour les accès distants et les systèmes critiques, révocation des accès dans les 24 heures suivant un départ

Sécurité opérationnelle : gestion des correctifs avec délai maximum de déploiement selon la criticité, protection antivirus/EDR sur tous les postes, journalisation et surveillance des événements de sécurité

Continuité d'activité : plan de continuité d'activité testé annuellement, sauvegardes testées mensuellement, procédure de gestion de crise cyber documentée

Relations avec les tiers : clauses de sécurité contractuelles avec les fournisseurs et sous-traitants ayant accès aux systèmes ou aux données de l'entreprise, audit de sécurité des accès tiers

La constitution du dossier de preuves pour l'assessment AirCyber Silver requiert une documentation précise et datée pour chaque mesure : politiques et procédures signées avec date de dernière révision, listes de diffusion des formations avec émargements, rapports de tests de sauvegarde et de continuité, captures d'écran des configurations de sécurité des outils déployés, et journaux des revues d'accès effectuées. La qualité et la complétude de cette documentation est aussi importante que la mise en oeuvre technique des mesures pour obtenir une évaluation favorable lors de l'assessment par l'assesseur accrédité.

Planification de la Transition Bronze vers Silver : Feuille de Route

La planification de la transition AirCyber Bronze vers Silver doit commencer par un gap analysis approfondi comparant l'état actuel de l'entreprise aux 39 mesures du niveau Silver, pour identifier les mesures déjà en place (qui nécessiteront seulement une documentation formalisée), les mesures partiellement implémentées (qui nécessiteront des ajustements), et les mesures absentes (qui nécessiteront un projet complet de mise en oeuvre).

La feuille de route typique pour la transition Bronze vers Silver sur 12 mois :

Mois 1-2 : Gap analysis et priorisation : inventaire complet des mesures Silver, identification des écarts avec l'état actuel, évaluation des ressources nécessaires (budget, compétences, temps) et définition du plan d'action priorisé selon l'effort et l'impact

Mois 3-6 : Mise en oeuvre des mesures techniques : déploiement MFA pour les accès distants, mise en place de la gestion des correctifs avec délais définis, déploiement d'un EDR sur tous les postes, configuration de la journalisation centralisée et activation de l'antivirus managé

Mois 5-8 : Documentation et formalisation : rédaction de la politique de sécurité, des procédures opérationnelles, des plans de continuité et des clauses contractuelles tiers ; organisation et documentation des formations de sensibilisation

Mois 9-11 : Tests et validation interne : test complet du plan de continuité, test de restauration depuis les sauvegardes, revue des accès utilisateurs et tiers, audit interne simulant les conditions de l'assessment Silver

Mois 12 : Assessment AirCyber Silver : soumission du dossier de candidature à l'assesseur accrédité, planification et conduite de l'assessment avec présentation des preuves de mise en oeuvre pour chaque mesure du niveau Silver

Le budget typique pour une PME de 50 à 200 employés cherchant à atteindre le niveau Silver est estimé entre 30 000 et 80 000 euros sur 12 mois, incluant les licences logicielles (EDR, MFA, sauvegarde managée), les éventuels prestations de conseil et d'assistance technique, et les coûts d'assessment. Ce niveau d'investissement est souvent partiellement éligible aux dispositifs d'aide à la cybersécurité des PME proposés par l'ANSSI, Bpifrance et les régions dans le cadre des plans de soutien à la cybersécurité de la chaîne d'approvisionnement aéronautique.

Maintien de la Certification AirCyber Silver : Surveillance Continue et Audits

L'obtention de la certification AirCyber Silver n'est pas la fin du parcours de conformité mais le début d'un cycle de maintien qui nécessite une surveillance continue et des audits de renouvellement réguliers. Le référentiel AirCyber prévoit des évaluations de renouvellement tous les deux ans, ainsi que la mise à jour obligatoire du dossier de preuves en cas de changement significatif du système d'information ou des pratiques de sécurité de l'organisation certifiée.

Les activités de maintien indispensables pour conserver le niveau Silver entre deux assessments :

Revue annuelle de la politique de sécurité : mettre à jour la politique de sécurité de l'information pour refléter les évolutions du système d'information, les nouvelles menaces identifiées et les retours d'expérience des incidents survenus dans l'intervalle

Tests de continuité et de sauvegarde : conduire au minimum un test complet de restauration depuis les sauvegardes tous les 6 mois et un test du plan de continuité d'activité une fois par an, en documentant les résultats et en traitant les anomalies identifiées

Revue des accès utilisateurs et tiers : réviser trimestriellement la liste des comptes utilisateurs actifs, des accès tiers accordés et des permissions applicatives pour détecter et révoquer les accès obsolètes ou excessifs

Veille sur le référentiel AirCyber : surveiller les mises à jour du référentiel publiées par le GIFAS et le groupe sectoriel AirCyber pour anticiper les nouvelles exigences qui pourraient s'appliquer lors du prochain assessment de renouvellement

Traçabilité des incidents de sécurité : documenter systématiquement tous les incidents de sécurité survenus (même mineurs), leur traitement et les mesures correctives prises, constituant un registre d'incidents utilisable lors des assessments pour démontrer l'efficacité des processus de réponse aux incidents

La valeur commerciale de la certification AirCyber Silver est croissante dans la chaîne d'approvisionnement aéronautique française et européenne. Les donneurs d'ordres majeurs (Airbus, Safran, Thales) intègrent de plus en plus les niveaux AirCyber dans leurs critères de qualification et d'homologation des fournisseurs, rendant la certification non seulement un outil de sécurité mais un avantage concurrentiel direct pour les PME et ETI qui ambitionnent de remporter ou de maintenir des contrats dans ce secteur exigeant.

AirCyber Silver dans le Contexte de la Conformité NIS 2 et ISO 27001

Le référentiel AirCyber, développé par le GIFAS (Groupement des Industries Françaises Aéronautiques et Spatiales) en coordination avec l'ANSSI et les grands donneurs d'ordres aéronautiques, s'inscrit dans un contexte réglementaire plus large où la cybersécurité de la chaîne d'approvisionnement devient une priorité réglementaire en Europe. La directive NIS 2 impose aux entités essentielles d'exiger de leurs fournisseurs des mesures de sécurité adéquates, et les grands donneurs d'ordres aéronautiques utilisent AirCyber comme outil de vérification de la maturité cybersécurité de leurs sous-traitants.

La complémentarité entre AirCyber Silver et ISO 27001 est significative : les 39 mesures du niveau Silver couvrent un sous-ensemble important des contrôles de l'Annexe A d'ISO 27001:2022, rendant la démarche AirCyber Silver une étape préparatoire efficace vers la certification ISO 27001 complète pour les PME qui souhaitent progresser vers ce niveau de maturité supérieur reconnu internationalement. Les organisations certifiées ISO 27001 disposant d'un SMSI opérationnel peuvent généralement passer l'assessment AirCyber Silver avec un effort documentaire minimal, car la majorité des exigences sont déjà satisfaites et documentées dans leur système de management.

Les PME aéronautiques qui anticipent les exigences contractuelles futures en obtenant le niveau Silver dès aujourd'hui se positionnent favorablement pour les appels d'offres des années 2025-2030, période pendant laquelle les donneurs d'ordres devraient systématiquement exiger des niveaux de certification AirCyber minimaux pour tous les fournisseurs accédant à leurs systèmes d'information ou traitant des données techniques sensibles comme les plans, les spécifications et les données de certification des aéronefs. L'investissement dans la démarche AirCyber Silver représente donc non seulement un renforcement de la posture de sécurité mais aussi un actif commercial durable dans un secteur de plus en plus sensible aux risques cybernétiques liés à la chaîne d'approvisionnement mondiale.

La démarche AirCyber s'inscrit dans une tendance de fond de l'industrie aéronautique mondiale vers une plus grande transparence et une meilleure gouvernance de la cybersécurité dans les chaînes d'approvisionnement globales, en réponse à la multiplication des attaques ciblant les fournisseurs comme porte d'entrée vers les donneurs d'ordres. Les PME et ETI qui s'engagent tôt dans cette démarche de certification bénéficient d'un avantage compétitif durable par rapport aux

concurrents qui retardent leur mise en conformité, tout en développant une culture interne de la sécurité qui génère des bénéfices opérationnels au-delà du seul maintien des contrats aéronautiques. L'accompagnement par un prestataire de sécurité expérimenté en réglementation aéronautique peut réduire significativement le temps et le coût de la démarche de certification en ciblant les actions à plus fort impact et en évitant les erreurs courantes dans la constitution du dossier de preuves. La démarche vers AirCyber Silver est un investissement structurant qui transforme l'approche de la cybersécurité au sein de l'entreprise, en passant d'une sécurité ad hoc à un système de management formel et documenté. Au-delà de la certification elle-même, ce processus développe des compétences internes, améliore les pratiques opérationnelles et renforce la confiance des partenaires commerciaux dans la capacité de l'entreprise à protéger les informations sensibles qui lui sont confiées dans le cadre de la collaboration industrielle aéronautique. Les bénéfices de la certification AirCyber Silver s'étendent bien au-delà du seul maintien des contrats avec les donneurs d'ordres exigeants. La certification AirCyber Silver donne accès à un réseau d'entreprises certifiées au sein de la filière aéronautique française, facilitant les échanges de bonnes pratiques et la veille sur les nouvelles menaces ciblant le secteur, complétant ainsi les bénéfices purement techniques et commerciaux de la démarche de certification par une dimension collaborative et communautaire précieuse.

