AirCyber Bronze Safran : Guide Complet Fournisseurs

> Depuis juin 2024, Safran impose AirCyber Bronze à tous ses fournisseurs. Délais, risques de déréférencement et 3 étapes immédiates pour vous conformer.

Depuis **juin 2024**, *Safran* — l'un des trois premiers groupes aéronautiques et de défense mondiaux, co-fondateur de BoostAerospace avec Airbus, Dassault Aviation et Thales — impose formellement la **labellisation AirCyber Bronze** à l'ensemble de ses fournisseurs directs dans le cadre de son programme de sécurisation de la supply chain *SAFe* (Safran Fournisseurs). Cette décision marque un tournant majeur pour la filière aéronautique française : pour la première fois, un donneur d'ordres de premier rang conditionne explicitement la poursuite des relations commerciales à l'obtention d'un label de cybersécurité, et non plus simplement à une auto-déclaration de conformité. Voici ce que cela signifie concrètement pour votre entreprise en tant que fournisseur, quels sont les risques réels en cas de non-conformité persistante, et quelles sont les trois actions immédiates à engager sans délai pour vous conformer à cette nouvelle exigence contractuelle.

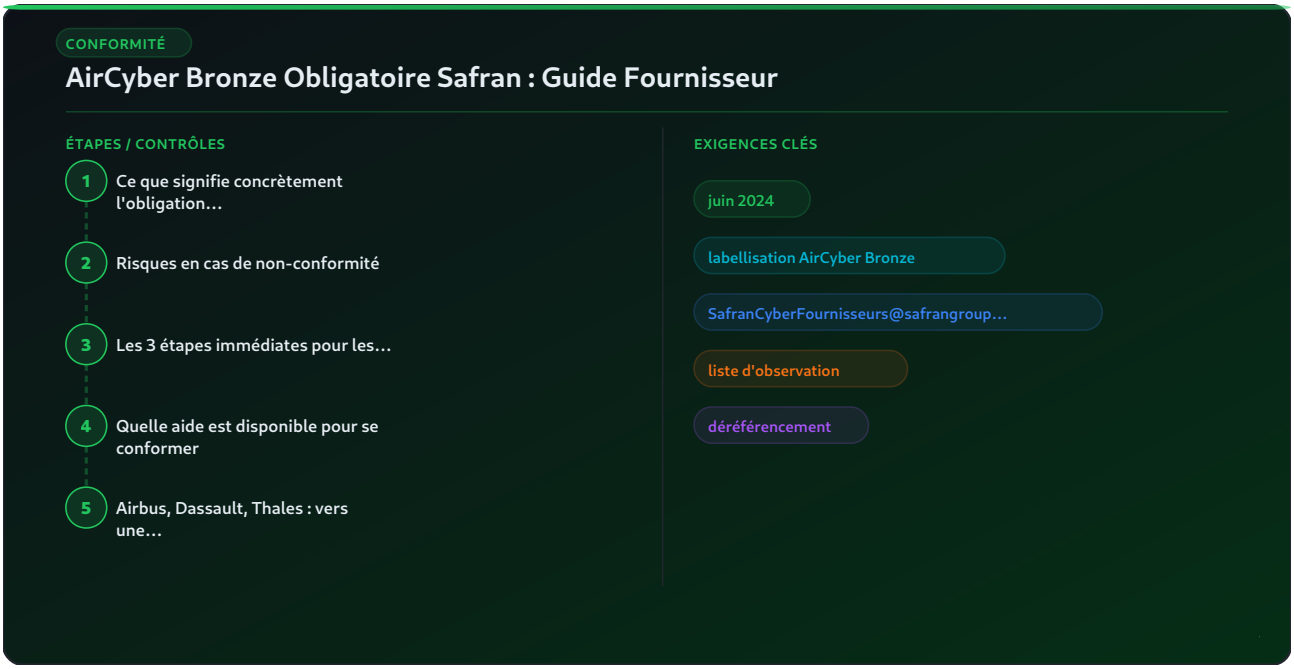
Points clés à retenir

- 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

À RETENIR

À retenir

AirCyber Bronze est désormais une condition contractuelle chez Safran. Le contact officiel du programme est SafranCyberFournisseurs@safrangroup.com. Ne pas engager la démarche dans les délais impartis expose au risque de déréférencement et de perte de contrats. Des subventions couvrant jusqu'à 70 % des coûts sont disponibles.



Ce que signifie concrètement l'obligation Safran AirCyber Bronze

Le programme **SAFe** (Safran Fournisseurs) traduit la volonté du groupe de sécuriser l'ensemble de sa chaîne d'approvisionnement contre les cybermenaces. Avec plus de 12 000 fournisseurs dans 60 pays, Safran est conscient que sa propre sécurité dépend de celle de ses partenaires — une compromission chez un sous-traitant peut permettre à un attaquant d'atteindre les systèmes de Safran via un mouvement latéral.

⚡ **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.

Concrètement, l'obligation signifie que vos acheteurs Safran peuvent désormais vous demander à tout moment de justifier de votre niveau AirCyber. Le programme a été officiellement notifié aux fournisseurs par courrier en **juin 2024**, avec des délais de mise en conformité qui varient selon le niveau de criticité de votre fourniture. Le contact officiel pour toute question relative au programme est : **SafranCyberFournisseurs@safrangroup.com**.

Les fournisseurs sont généralement classés en trois catégories de criticité, déterminant les délais accordés : fournisseurs *critiques* (accès aux SI Safran, fournitures de sécurité) — délai court ; fournisseurs *importants* (composants majeurs) — délai intermédiaire ; fournisseurs *standards* — délai plus long. Si vous n'avez pas encore été notifié, contactez directement votre acheteur Safran ou le programme SAFe pour connaître votre classification.

Risques en cas de non-conformité

Les conséquences d'une non-conformité à l'obligation AirCyber Bronze chez Safran sont graduées mais potentiellement sévères.

Dans un premier temps, votre entreprise peut être placée en **liste d'observation**, avec un plan d'actions exigé et des visites de suivi. Si aucune démarche n'est engagée, le risque de

déréférencement (exclusion du panel fournisseurs) est réel. Dans les appels d'offres, les entreprises non labellisées peuvent se voir disqualifiées au stade de la qualification fournisseur. Enfin, une cyberattaque touchant votre entreprise et se propageant à Safran pourrait engager votre responsabilité contractuelle si vous n'aviez pas respecté vos obligations de sécurité.

Il est important de noter que Safran n'est pas seul dans cette démarche. **Airbus**, **Dassault Aviation** et **Thales** — les trois autres fondateurs de BoostAerospace — ont tous intégré AirCyber dans leurs grilles d'évaluation fournisseurs et s'orientent vers des obligations similaires. Être labellisé Bronze protège donc vos relations commerciales avec l'ensemble de la filière, pas seulement avec Safran.

Les 3 étapes immédiates pour les fournisseurs Safran

Si vous êtes fournisseur Safran et n'avez pas encore engagé votre démarche AirCyber, voici les trois actions à mener en priorité absolue.

Étape 1 — Contactez le programme SAFe et clarifiez votre délai

Écrivez à **SafranCyberFournisseurs@safrangroup.com** en indiquant votre numéro de fournisseur et en demandant votre classification et le délai qui vous est accordé. Conservez toutes les communications écrites. Cette démarche proactive est bien perçue par les acheteurs Safran et peut vous accorder du temps supplémentaire.

Étape 2 — Réalisez l'auto-évaluation AirCyber

Accédez au portail BoostAerospace AirCyber et complétez le questionnaire d'auto-évaluation. Ce bilan initial vous donnera une image claire de votre niveau de maturité actuel et des écarts à combler. Planifiez cette auto-évaluation dans les **deux semaines** suivant la réception de votre notification Safran.

Étape 3 — Lancez votre plan de remédiation et cherchez des financements

Sur la base de l'auto-évaluation, établissez un plan de remédiation priorisé et identifiez les financements disponibles. Le diagnostic AirCyber coûte environ **8 800 € HT**, subventionnable à 50 % via France Relance. France 2030 Cyber PME permet d'obtenir jusqu'à 70 % des dépenses de sécurisation. Consultez notre article détaillé sur les financements AirCyber disponibles pour les PME.

Quelle aide est disponible pour se conformer

La filière aéronautique a mis en place plusieurs dispositifs d'aide pour faciliter la mise en conformité des PME. Le **GIFAS** (Groupement des Industries Françaises Aéronautiques et Spatiales) et l'**UIMM** proposent des accompagnements mutualisés permettant à plusieurs PME de partager les coûts d'un assesseur ou d'une formation.

Les clusters régionaux — **Aerospace Valley** (Nouvelle-Aquitaine/Occitanie) et **Normandie AeroEspace** — organisent régulièrement des sessions collectives d'information et de préparation à AirCyber. Ces événements sont souvent gratuits pour les membres et permettent de rencontrer des assesseurs accrédités.

Notre équipe propose un accompagnement AirCyber spécifiquement adapté aux fournisseurs Safran, avec une connaissance approfondie des exigences SAFe et des délais à respecter. Retrouvez toutes nos ressources dans le centre de ressources AirCyber, incluant le guide complet de la labellisation Bronze.

Pour préparer votre audit, consultez la checklist des 44 mesures ANSSI et la liste des documents obligatoires pour l'audit.

Le référentiel Guide d'Hygiène Informatique de l'ANSSI est téléchargeable gratuitement et constitue la base technique des 44 mesures Bronze.

Airbus, Dassault, Thales : vers une obligation similaire ?

La question est sur toutes les lèvres dans la supply chain. La réponse courte est : **oui, c'est une tendance de fond irréversible**. Airbus a intégré AirCyber dans son programme *AirSupply* de qualification fournisseurs. Dassault Aviation évalue ses fournisseurs sur la base du référentiel AirCyber depuis 2022. Thales pousse ses fournisseurs vers AirCyber dans le cadre de son programme *Cyber@TS*.

Depuis la reconnaissance d'AirCyber comme référentiel mondial par l'**Aviation ISAC** en septembre 2023 à Dublin, la pression internationale s'ajoute à la pression domestique. Les donneurs d'ordres américains (Boeing, Lockheed Martin, Raytheon) commencent à référencer AirCyber comme équivalent au *CMMC* (Cybersecurity Maturity Model Certification) américain pour leurs fournisseurs européens.

FAQ — AirCyber Bronze et obligation Safran

Mon entreprise a 12 salariés, suis-je vraiment concerné par l'obligation Safran ?

Oui. L'obligation Safran s'applique à tous les fournisseurs directs, quelle que soit leur taille. Il n'existe pas d'exemption pour les TPE ou les microentreprises. Cependant, les *mesures AirCyber Bronze* sont dimensionnées pour être accessibles même aux très petites entreprises, et les financements disponibles (France Relance, France 2030) s'appliquent aux entreprises jusqu'à 90 M€ de CA, donc couvrent la quasi-totalité des fournisseurs concernés.

Quel délai réaliste pour obtenir le Bronze si je commence aujourd'hui ?

En partant de zéro, le processus complet prend de **3 à 6 mois** : auto-évaluation (2 semaines), plan de remédiation (1 à 2 semaines), mise en œuvre des mesures (2 à 4 mois), puis audit par l'assesseur (planning à anticiper car les assesseurs sont souvent bookés 4 à 8 semaines à

l'avance). Si votre entreprise a déjà une démarche de sécurité en place (ISO 27001, PSSI existante, etc.), ce délai peut être réduit à 2 à 3 mois.

Que se passe-t-il si je ne l'obtiens pas avant le délai Safran ?

Si vous êtes engagé dans la démarche et pouvez le prouver (auto-évaluation réalisée, plan de remédiation formalisé, assesseur mandaté), Safran accordera généralement un délai supplémentaire. Ce qui est rédhibitoire, c'est l'absence totale de démarche. Dans ce cas, le risque de déréférencement dans les prochains appels d'offres est réel. Communiquez proactivement avec votre acheteur Safran et le programme SAFe pour montrer votre engagement.

Mise en œuvre pratique : étapes et livrables

La conformité réglementaire génère une documentation substantielle qui doit être maintenue à jour et accessible lors des audits. Une organisation structurée de ces livrables simplifie considérablement les exercices de conformité et réduit le temps consacré à leur préparation.

Livrables documentaires essentiels

Quel que soit le référentiel de conformité concerné, les livrables fondamentaux incluent : un registre des traitements (obligatoire RGPD, utile pour tout SMSI) maintenu par le DPO ou le RSSI ; une politique de sécurité de l'information (PSI ou PSSI) approuvée par la direction et diffusée à tous les collaborateurs ; des procédures opérationnelles documentées pour les

processus critiques (gestion des incidents, accès privilégiés, sauvegardes) ; un plan de continuité d'activité (PCA) testé annuellement ; et des rapports d'audit internes et de revue de direction formalisés. Ces documents constituent le «squelette» du SMSI et sont systématiquement vérifiés lors des audits de certification.

Gouvernance et responsabilités

La conformité réglementaire est un effort collectif qui ne peut pas reposer uniquement sur le RSSI ou le DPO. Une gouvernance efficace définit clairement les rôles : le COMEX assume la responsabilité globale de la conformité (risque financier et réputationnel) ; les DSI et RSSI mettent en œuvre les mesures techniques ; les métiers identifient les données et processus critiques à protéger ; et les DPO/compliance officers assurent la cohérence réglementaire. Les comités de sécurité trimestriels, impliquant toutes ces parties prenantes, garantissent l'alignement entre les exigences réglementaires et les capacités opérationnelles de l'organisation. Le suivi des actions de remédiation dans un outil de GRC (Governance, Risk & Compliance) formalise ce processus et facilite la production des preuves d'audit.

Sanction et contrôle : ce que les autorités vérifient

Comprendre les priorités de contrôle des autorités de régulation permet aux organisations de concentrer leurs efforts sur les domaines qui font l'objet d'une surveillance accrue. Les autorités de supervision (CNIL, ANSSI, ACP pour le secteur bancaire, HAS pour le secteur santé) publient régulièrement leurs priorités de contrôle.

Priorités de contrôle 2025-2026

Les domaines prioritaires identifiés par les autorités françaises pour 2025-2026 : la sécurité des données de santé (contrôles HDS en forte augmentation suite aux incidents hospitaliers) ; l'IA et le traitement des données personnelles (CNIL a annoncé 300 mises en demeure liées à l'IA en 2025) ; les sous-traitants et tiers (vérification des DPA et des audits de sécurité des fournisseurs) ;

et la notification des violations de données dans les délais légaux (72h RGPD, 24h NIS 2 pour les entités essentielles). Les organisations qui documentent proactivement leur conformité dans ces domaines réduisent significativement leur exposition aux sanctions et bénéficient généralement d'une procédure d'audit moins contraignante.

Programme de préparation aux audits

Un programme structuré de préparation aux audits réduit le stress et améliore les résultats. Douze mois avant un audit de certification : gap analysis interne pour identifier les non-conformités. Six mois avant : corrections des écarts majeurs et préparation de la documentation. Trois mois avant : audit blanc interne conduit par un consultant externe indépendant. Un mois avant : formation des équipes sur les procédures et livrables à présenter. Cette approche systématique, validée par des centaines d'organisations certifiées ISO 27001, transforme l'audit de certification d'une épreuve redoutée en une validation formelle d'un travail déjà accompli.

Synthèse et feuille de route conformité

La conformité réglementaire est un processus continu, non un projet ponctuel. Les organisations qui abordent ISO 27001, NIS 2, RGPD ou HDS comme des certifications à obtenir une fois pour toutes échouent systématiquement lors des audits de renouvellement. La clé du succès est l'intégration des exigences réglementaires dans les processus opérationnels quotidiens, non leur traitement comme des obligations externes.

En pratique, les organisations matures en matière de conformité fonctionnent avec un SMSI vivant : des revues de direction trimestrielles, un audit interne annuel, des exercices de gestion de crise bi-annuels, et une veille réglementaire hebdomadaire. Le coût de la conformité maintenue en continu est significativement inférieur au coût d'une remise à niveau précipitée avant un audit ou une notification de violation. Les amendes CNIL, les pénalités NIS 2, et les pertes de contrats liées à une non-conformité documentée représentent des risques financiers et réputationnels mesurables que la gouvernance de direction doit intégrer dans l'analyse des risques métier.

Points d'attention avancés pour les auditeurs et RSSI

Au-delà de la conformité de surface, les auditeurs expérimentés et les RSSI cherchent à évaluer la robustesse réelle du dispositif de sécurité. Ce niveau d'analyse requiert de dépasser la vérification documentaire pour s'intéresser à l'efficacité opérationnelle des contrôles.

Pièges courants dans les audits de conformité

Plusieurs patterns d'échec reviennent régulièrement lors des audits de renouvellement. La conformité sur papier sans effectivité opérationnelle : des politiques formalisées mais non appliquées, des procédures documentées mais inconnues des équipes, des contrôles déclarés actifs mais non supervisés. La dérive post-certification : les organisations qui traitent la certification comme une fin en soi plutôt que comme un jalons d'un processus continu connaissent systématiquement une dégradation de leur posture sécurité entre deux audits. La gestion insuffisante des tiers : plus de 60% des violations impliquent un fournisseur ou un prestataire, mais les contrats de sous-traitance et les audits tiers sont souvent les parents pauvres des programmes de conformité. Adresser ces trois points avant l'audit réduit significativement le risque de non-conformité majeure.

Métriques de maturité à présenter en audit

Les auditeurs modernes s'intéressent aux indicateurs de fonctionnement réel du SMSI plutôt qu'à la simple existence des documents. Préparer : statistiques de gestion des incidents sur 12 mois (nombre, délai de traitement, taux de récidive) démontrant une amélioration continue ; résultats des exercices de continuité avec les actions correctives entreprises ; données de sensibilisation (taux de participation aux formations, taux d'échec aux simulations de phishing) ; et résultats des audits internes avec suivi des actions de remédiation. Ces métriques transforment l'audit en démonstration de la maturité de l'organisation plutôt qu'en exercice de conformité documentaire, et constituent la meilleure défense contre les questions inattendues des auditeurs sur l'efficacité opérationnelle des contrôles.

Checklist de mise en œuvre et points de contrôle

La mise en pratique des recommandations de cet article nécessite une approche structurée. Cette checklist synthétise les points de contrôle essentiels pour évaluer l'état d'avancement de votre déploiement et identifier les actions prioritaires.

Phase de préparation et d'inventaire

Avant toute action technique, constituer un inventaire précis est indispensable. Les éléments à recenser : cartographie exhaustive des actifs concernés (systèmes, applications, flux de données) avec leur criticité métier associée ; identification des propriétaires techniques et fonctionnels pour chaque actif ; évaluation du niveau de maturité actuel à partir des référentiels reconnus (CIS Controls, ISO 27001, NIST CSF) ; et documentation des dépendances entre composants pour anticiper les impacts des modifications. Un inventaire incomplet génère des angles morts qui deviennent des vecteurs d'attaque exploitables par des acteurs malveillants disposant d'informations accessibles publiquement (OSINT, Shodan, LinkedIn).

Phase de déploiement et validation

Le déploiement progressif réduit les risques d'interruption de service et facilite la détection des régressions. Adopter un modèle de déploiement par vagues (wave deployment) : d'abord les environnements de développement et de test pour valider les configurations, ensuite les systèmes non-critiques en production, enfin les systèmes critiques lors de fenêtres de maintenance planifiées. Chaque vague s'accompagne d'une validation fonctionnelle complète et d'une période d'observation des métriques de performance et de sécurité. Un plan de retour arrière documenté et testé est obligatoire avant toute opération sur un système critique. Les critères de succès doivent être définis avant le déploiement, non après — un taux de faux positifs inférieur à 5% pour les alertes de sécurité, une disponibilité maintenue au niveau SLA contractuel, et l'absence d'incidents de sécurité liés aux modifications.

Phase de supervision et d'amélioration continue

La mise en place d'indicateurs de suivi permet de mesurer l'efficacité des mesures déployées et de justifier leur maintien auprès de la direction. Tableau de bord mensuel recommandé : nombre d'alertes générées par catégorie (critique, majeur, mineur) avec tendance sur 6 mois ; taux de couverture des actifs critiques par les contrôles de sécurité ; délai moyen de remédiation des vulnérabilités par sévérité CVSS ; et résultats des tests de régression mensuels sur les règles de détection. Ce tableau de bord, présenté en comité de sécurité, constitue la base d'un dialogue constructif entre les équipes techniques et le management sur les priorités d'investissement en cybersécurité.

Ressources, outils et veille spécialisée

L'efficacité opérationnelle des équipes de sécurité repose sur la maîtrise des outils adaptés et sur une veille continue sur les évolutions techniques et réglementaires du domaine. Ce panorama recense les ressources incontournables pour approfondir les sujets abordés dans cet article.

Outils open source recommandés

L'écosystème open source de la cybersécurité offre des outils de qualité professionnelle, souvent comparables voire supérieurs aux solutions commerciales sur des cas d'usage spécifiques. Pour la détection et la réponse à incident : OSSEC/Wazuh (HIDS/XDR open source déployé sur plus de 500 000 systèmes), TheHive et Cortex (orchestration et automatisation de la réponse à incident), MISP (partage de threat intelligence, utilisé par plus de 6 000 organisations mondiales). Pour l'analyse forensique : Autopsy (interface graphique pour Sleuth Kit, analyse disque), Volatility 3 (analyse mémoire vive), YARA (création de règles de détection de malwares). Pour l'audit d'infrastructure : OpenSCAP (compliance scanning automatisé), Lynis (audit de durcissement Linux), BloodHound (cartographie des chemins d'attaque Active Directory). Ces outils, maintenus par des communautés actives et adoptés par les grandes entreprises et agences gouvernementales, constituent le socle technique des équipes SOC modernes.

Sources de veille et formation continue

La cybersécurité évolue à un rythme qui impose une veille structurée pour maintenir l'efficacité des défenses. Les sources primaires à surveiller : CERT-FR (bulletins d'alerte et de sensibilisation de l'ANSSI, à intégrer dans les flux de veille en priorité) ; NVD et CISA KEV (catalogue des CVE et des vulnérabilités activement exploitées) ; Microsoft MSRC, Google Project Zero et Cisco Talos (recherche offensive et advisories éditeurs) ; et les publications académiques des conférences SSTIC (France), USENIX Security, IEEE S&P et CCS. Pour la montée en compétences des équipes, les certifications SANS GIAC (GCIH, GPEN, GCFA) offrent le meilleur équilibre entre reconnaissance professionnelle et valeur pratique. Les plateformes d'entraînement TryHackMe et HackTheBox permettent une pratique régulière sur des scénarios réalistes sans risque légal, avec des modules spécifiques adaptés aux profils défensifs (Blue Team Labs) et offensifs (HTB Pro Labs).