AirCyber vs ISO 27001 : Différences et Complémentarité

> AirCyber vs ISO 27001 : différences clés pour sous-traitant aéronautique. Quelle certification prioriser ? Comment combiner les deux pour viser Gold ?

Pour une **PME sous-traitante de l'industrie aéronautique**, le choix entre la labellisation *AirCyber* et la certification *ISO 27001* est une décision stratégique qui engage plusieurs années d'effort et des budgets significatifs. Ces deux référentiels de cybersécurité partagent des objectifs communs — protéger le système d'information et démontrer la maturité sécurité à ses clients — mais leur périmètre, leurs exigences et leur reconnaissance sectorielle diffèrent fondamentalement. Comprendre ces différences permet d'éviter des erreurs coûteuses et de construire une feuille de route cohérente avec les attentes des donneurs d'ordre comme Airbus, Dassault Aviation, Safran ou Thales. En 2024, **plus de 430 membres** de la filière aéronautique et spatiale française ont rejoint le programme AirCyber lancé par BoostAerospace, démontrant que cette labellisation est devenue un prérequis incontournable pour accéder aux marchés sensibles. Ce guide comparatif détaille les critères essentiels pour orienter votre choix et maximiser la valeur de vos investissements en cybersécurité.

Tableau comparatif : AirCyber Bronze vs ISO 27001

Le tableau suivant synthétise les différences structurelles entre les deux référentiels sur les critères qui importent le plus aux PME aéronautiques :

Critère	AirCyber Bronze	ISO 27001
Périmètre	44 mesures techniques et organisationnelles ANSSI + mesures sectorielles aéro	114 contrôles (Annexe A), SMSI complet, périmètre libre
Coût estimé PME 50 sal.	15 000 – 35 000 €	50 000 – 150 000 €
Durée typique	3 – 6 mois	12 – 24 mois
Obligation contractuelle	Croissante : clauses supply chain Airbus, Dassault	Requise sur certains marchés défense/espace
Reconnaissance	Aviation ISAC mondial (Dublin 2023), filière FR	Internationale, tous secteurs
Organisme d'audit	Assesseurs accrédités BoostAerospace	Organismes accrédités COFRAC / UKAS
Renouvellement	Annuel (Bronze), 3 ans (Silver/Gold)	3 ans (audits de surveillance annuels)

Pourquoi AirCyber n'est pas un sous-ensemble d'ISO 27001

Une idée reçue très répandue consiste à penser qu'AirCyber Bronze serait simplement une version simplifiée d'ISO 27001 adaptée à l'aéronautique. C'est une erreur d'analyse. Les deux référentiels ont des **ADN fondamentalement différents**.

> ⚡ **Retour terrain**
>
> Lors d'un accompagnement ISO 27001 pour un hébergeur de données de santé, l'audit de certification a identifié un écart sur le contrôle A.12.4 (journalisation) : les logs d'accès administrateur n'étaient pas centralisés et certains étaient stockés localement sur les serveurs eux-mêmes — effaçables par un admin compromis. La correction a pris 3 semaines ; l'audit de certification avait été planifié 2 semaines après. Leçon : toujours faire un pre-audit interne complet 6 semaines avant la date officielle.

ISO 27001 est un système de management généraliste : il exige la mise en place d'un *SMSI* (Système de Management de la Sécurité de l'Information) avec des processus de gouvernance, une politique documentée, des cycles Plan-Do-Check-Act, et une certification par un organisme accrédité indépendant. Le périmètre est défini librement par l'entreprise, ce qui permet de certifier uniquement une partie du SI — mais aussi de "contourner" certains actifs critiques.

AirCyber Bronze intègre des mesures sectorielles spécifiques à l'aéronautique absentes d'ISO 27001, notamment :

La gestion de la **chaîne d'approvisionnement numérique** propre aux flux EDI et PLM aéronautiques

Les exigences de cloisonnement réseau liées aux systèmes embarqués et données ITAR/EAR

Les obligations de reporting vers le **CERT Aviation** (créé en novembre 2022 par 9 fondateurs de la filière)

L'alignement sur les standards ANSSI Guide d'hygiène informatique, directement référencés dans le questionnaire Bronze

AirCyber Silver couvre déjà la quasi-totalité d'ISO 27001

À l'inverse, le niveau **Silver AirCyber représente une couverture quasi-complète d'ISO 27001**. Avec ses exigences calquées sur la norme internationale, Silver impose un SMSI structuré, une gestion documentaire formalisée et une revue de direction annuelle. Les **~28 entreprises** ayant atteint le niveau Silver en France disposent de facto d'une base solide pour obtenir ISO 27001 avec un investissement incrémental limité.

Concrètement, une entreprise certifiée Silver AirCyber devra compléter environ 15 à 20% de contrôles supplémentaires pour atteindre ISO 27001, principalement sur la **gestion des actifs physiques** et les exigences formelles de l'accréditation COFRAC.

Quelle certification prioriser pour une PME aéronautique ?

La réponse dépend de votre situation contractuelle et de votre horizon stratégique. Voici notre recommandation par profil :

→ **Prioriser AirCyber Bronze si :** vos clients directs l'exigent ou vont l'exiger dans les 12 à 18 prochains mois, si vous êtes une PME de moins de 100 salariés avec un SI de taille raisonnable, ou si vous cherchez la démonstration la plus rapide de maturité cyber dans la filière aéronautique.

→ **Envisager ISO 27001 directement si :** vous visez des marchés hors aéronautique (cybersécurité industrielle, défense multi-sectorielle), si un client non-aéronautique l'impose contractuellement, ou si votre stratégie commerciale cible l'international hors filière BoostAerospace.

Dans la grande majorité des cas, **la séquence optimale est : Bronze AirCyber d'abord, puis Silver, puis ISO 27001 en parallèle si nécessaire**. Cette approche maximise la valeur de chaque investissement et réduit les redondances. Consultez notre page dédiée à l'accompagnement AirCyber pour évaluer votre situation.

Comment les deux certifications se complètent pour aller vers Gold

Le niveau **Gold AirCyber** (environ 194 questions, ~6% des membres) représente la convergence entre AirCyber Silver et les exigences d'un SMSI ISO 27001 complet. Les entreprises qui visent Gold disposent généralement déjà d'une certification ISO 27001 ou sont en cours d'obtention. La complémentarité devient alors maximale : les deux référentiels s'alimentent mutuellement, les audits peuvent être combinés, et les preuves documentaires sont partagées.

Cette synergie est particulièrement valorisée pour l'accès aux contrats de **défense et de spatial** où les exigences de sécurité cumulent les deux référentiels. Pour approfondir votre stratégie, visitez notre Centre de Ressources AirCyber qui centralise les guides pratiques et modèles documentaires.

À RETENIR

Points clés à retenir

✓ **AirCyber Bronze ≠ sous-ensemble ISO 27001** : des mesures sectorielles aéro sont spécifiques à AirCyber

✓ **AirCyber Silver ≈ ISO 27001** : couverture quasi-complète, transition facilitée

✓ **Séquence recommandée PME** : Bronze → Silver → ISO 27001 si contractuellement requis

✓ **NIS 2 renforce l'urgence** : les donneurs d'ordre vont exiger des preuves de maturité supply chain

✓ **Gold + ISO 27001** = combinaison optimale pour contrats défense/spatial

FAQ : AirCyber vs ISO 27001

Peut-on passer directement à AirCyber Silver sans Bronze ?

Techniquement oui, le programme AirCyber permet d'entrer directement au niveau Silver. Cependant, en pratique, la quasi-totalité des entreprises commence par Bronze pour maîtriser les bases avant de s'engager dans le processus Silver plus exigeant et plus coûteux. L'expérience de l'évaluation Bronze est également formative pour les équipes.

ISO 27001 est-elle reconnue dans la filière aéronautique française ?

ISO 27001 est reconnue et valorisée, mais elle ne remplace pas AirCyber pour les donneurs d'ordre de la filière BoostAerospace. Airbus, Dassault, Safran et Thales référencent spécifiquement AirCyber dans leurs clauses supply chain. ISO 27001 peut compléter AirCyber mais ne s'y substitue pas sur les marchés aéronautiques français.

Combien de temps faut-il pour passer de Bronze à Silver après avoir obtenu ISO 27001 ?

Si vous disposez d'une certification ISO 27001 active, le passage à Silver AirCyber est significativement accéléré : comptez 3 à 6 mois supplémentaires pour couvrir les mesures sectorielles aéronautiques spécifiques à AirCyber qui ne figurent pas dans ISO 27001. Votre documentation SMSI existante est directement réutilisable.

Articles complémentaires

→ Guide complet : obtenir la labellisation AirCyber Bronze

→ Checklist des 44 mesures ANSSI AirCyber Bronze

→ AirCyber Silver : exigences et feuille de route depuis Bronze

→ Financement AirCyber : subventions et aides pour PME

Besoin d'aide pour choisir votre stratégie de certification ?

Nos experts analysent votre situation contractuelle et définissent la feuille de route optimale Bronze → Silver → ISO 27001.

Obtenir un diagnostic gratuit →

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).

Retours d'expérience et scénarios concrets

Les incidents de sécurité documentés et les retours d'expérience de déploiements réels constituent une source d'apprentissage irremplaçable. Les cas présentés ici illustrent les défis pratiques rencontrés par des organisations lors de la mise en œuvre des mesures abordées dans cet article.

Leçons tirées d'incidents réels

L'analyse des incidents publiés dans les rapports sectoriels (Verizon DBIR, IBM X-Force, CrowdStrike Global Threat Report) révèle des patterns récurrents. Les violations de données les plus coûteuses partagent trois caractéristiques : un délai de détection long (moyenne de 194 jours selon le rapport IBM Cost of a Data Breach 2025), une phase de latéralisation étendue exploitant des comptes légitimes ou des failles de configuration, et une absence de segmentation réseau permettant aux attaquants d'atteindre les données sensibles depuis un premier point de compromission périphérique. La mise en œuvre des mesures décrites dans cet article cible

directement ces trois facteurs de risque, avec un impact mesurable sur les métriques MTTD (Mean Time To Detect) et MTTR (Mean Time To Respond).

Facteurs de succès et pièges à éviter

Les déploiements réussis partagent des facteurs communs : sponsorship exécutif clair avec budget dédié et KPIs définis dès le début du projet ; implication des équipes opérationnelles (NOC, SOC, métiers) dans la conception pour anticiper les contraintes pratiques ; approche phased évitant le big-bang qui génère des régressions difficiles à diagnostiquer ; et formation des équipes en parallèle du déploiement technique pour garantir l'adoption. À l'inverse, les projets qui échouent présentent systématiquement une ou plusieurs de ces caractéristiques : périmètre mal défini qui dérive au fil des mois (scope creep), défaut de communication avec les métiers sur les impacts opérationnels des mesures de sécurité, ou sous-estimation des ressources nécessaires à la maintenance post-déploiement. Un projet de sécurité livré dans les délais mais dont les équipes n'ont pas les moyens d'assurer la supervision quotidienne a une efficacité proche de zéro à six mois.