# Checklist 44 Mesures ANSSI : AirCyber Bronze Complet

> Checklist complète des 44 mesures ANSSI pour AirCyber Bronze : 8 domaines, contrôles détaillés et niveaux requis pour sous-traitants aéronautiques.

Obtenir la **labellisation AirCyber Bronze** passe nécessairement par la conformité aux 44 mesures du *Guide d'Hygiène Informatique* de l'ANSSI, complétées par des mesures sectorielles spécifiques à la filière aéronautique. Cette checklist opérationnelle, conçue pour les équipes techniques et les responsables sécurité des PME sous-traitantes, vous permet d'évaluer précisément votre niveau de conformité sur chacun des 8 domaines du référentiel, d'identifier les écarts prioritaires à combler avant la visite de l'assesseur et de structurer votre dossier documentaire de preuve. Elle est conçue pour être utilisée conjointement avec le guide complet d'obtention de la labellisation AirCyber Bronze et la liste des documents à préparer pour l'audit. Chaque domaine est annoté avec le niveau de priorité et le type de preuve documentaire attendu lors de l'audit par l'assesseur accrédité.

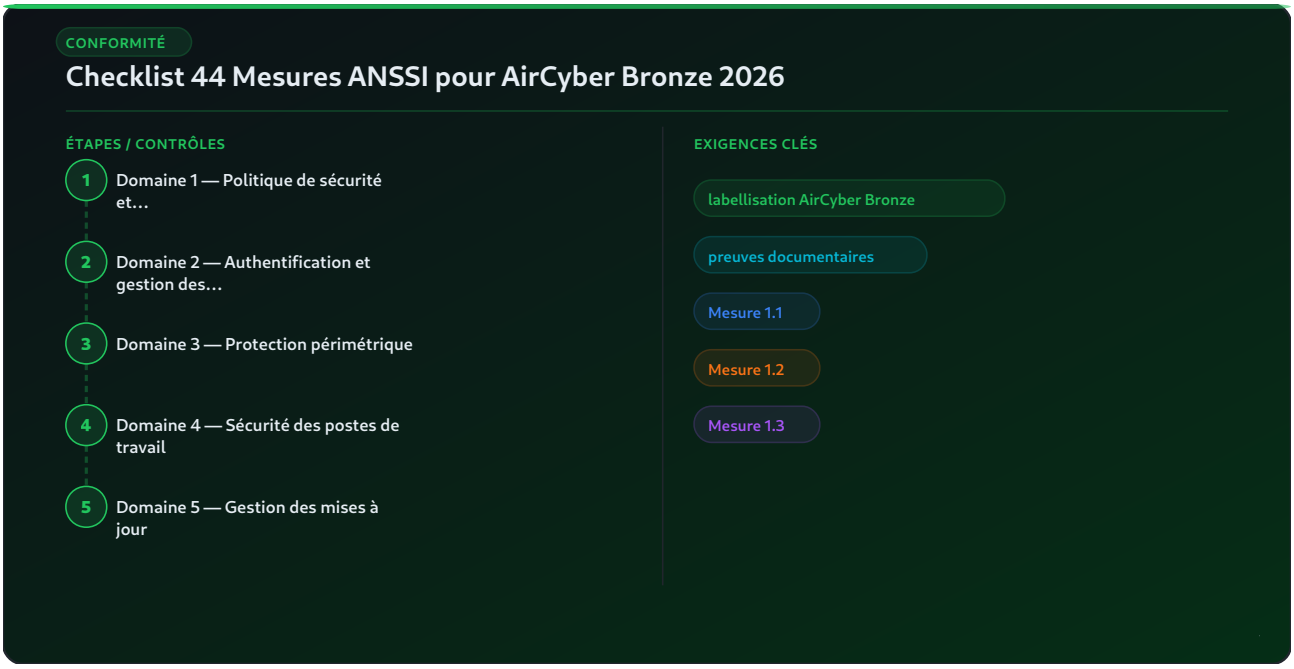
### Points clés à retenir

- 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

Les domaines Politique de sécurité, Authentification et Gestion des mises à jour sont les plus fréquemment défaillants lors des audits AirCyber Bronze. Concentrez votre effort initial sur ces trois domaines pour maximiser vos chances de succès au premier passage.




## Domaine 1 — Politique de sécurité et organisation

Ce domaine est le socle de toute démarche AirCyber. Sans documentation formalisée et validée par la direction, aucune autre mesure technique ne peut être correctement évaluée. L'assesseur attend des **preuves documentaires** (documents signés, datés, diffusés) et non de simples déclarations d'intention.

⚡ **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.

- ☐ **Mesure 1.1** — Définir une *PSSI* (Politique de Sécurité des Systèmes d'Information) formalisée, validée par la direction et communiquée à l'ensemble du personnel
- ☐ **Mesure 1.2** — Désigner un référent sécurité identifié (RSSI ou équivalent), avec une fiche de poste formalisée
- ☐ **Mesure 1.3** — Maintenir un inventaire exhaustif et à jour des actifs informatiques (matériels, logiciels, données)
- ☐ **Mesure 1.4** — Disposer d'une procédure formalisée de gestion des incidents de sécurité, avec escalade et notification
- ☐ **Mesure 1.5** — Intégrer des clauses de sécurité dans les contrats avec les prestataires et sous-traitants (dont la supply chain aéronautique)

## Domaine 2 — Authentification et gestion des accès

L'authentification est systématiquement l'un des domaines les plus défaillants lors des audits. Les comptes partagés, les mots de passe triviaux et l'absence de **MFA** sur les accès distants sont les écarts les plus couramment relevés. Ce domaine couvre la gestion du cycle de vie complet des comptes utilisateurs.

- ☐ **Mesure 2.1** — Appliquer une politique de mots de passe robuste : longueur minimale 12 caractères, complexité, historique des 10 derniers mots de passe
- ☐ **Mesure 2.2** — Imposer l'**authentification à deux facteurs (MFA)** pour tous les accès distants (VPN, RDP, SSH, webmail)
- ☐ **Mesure 2.3** — Appliquer le principe du *moindre privilège* : chaque utilisateur ne dispose que des droits strictement nécessaires à sa fonction
- ☐ **Mesure 2.4** — Interdire les comptes génériques ou partagés ; chaque compte doit être nominatif et tracé
- ☐ **Mesure 2.5** — Mettre en place une procédure de révocation immédiate des accès en cas de départ ou de changement de fonction (délai max : 24h)
- ☐ **Mesure 2.6** — Séparer les comptes administrateurs des comptes utilisateurs courants ; les admins ne naviguent pas sur Internet avec leurs comptes à privilèges

## Domaine 3 — Protection périmétrique

La *protection périmétrique* couvre la séparation entre le réseau interne de l'entreprise et Internet, ainsi que la segmentation interne entre zones de sécurité différentes. Dans un contexte

aéronautique, la protection des données **ITAR/EAR** (données techniques soumises à contrôle à l'exportation) renforce les exigences de cloisonnement.

- [ ] **Mesure 3.1** — Déployer un **pare-feu** correctement configuré entre Internet et le réseau interne, avec journalisation des flux bloqués
- [ ] **Mesure 3.2** — Segmenter le réseau : séparer au minimum le réseau de production, le réseau bureautique et la zone WiFi invités
- [ ] **Mesure 3.3** — Restreindre l'accès Internet aux seules destinations nécessaires pour l'activité (filtrage par catégorie ou liste blanche sur les postes critiques)
- [ ] **Mesure 3.4** — Sécuriser les accès distants via **VPN** avec chiffrement fort (TLS 1.2 minimum, IKEv2 recommandé)
- [ ] **Mesure 3.5** — Contrôler et enregistrer les flux entrants vers les services exposés sur Internet (serveur mail, portail web, API)

## Domaine 4 — Sécurité des postes de travail

Les postes de travail sont le premier vecteur d'attaque dans les PME industrielles. Ce domaine couvre la protection des terminaux (workstations, laptops, tablettes) utilisés pour traiter des données sensibles liées aux contrats aéronautiques.

- [ ] **Mesure 4.1** — Déployer une solution antivirus ou *EDR* (Endpoint Detection and Response) sur l'ensemble des postes, avec mises à jour automatiques des signatures
- [ ] **Mesure 4.2** — Chiffrer les disques durs de tous les postes nomades (laptops, tablettes) avec BitLocker ou équivalent
- [ ] **Mesure 4.3** — Restreindre l'utilisation des supports amovibles (clés USB) par politique de groupe ou solution MDM

- [ ] **Mesure 4.4** — Interdire l'installation de logiciels non autorisés sur les postes de travail (liste blanche ou politique UAC stricte)

## Domaine 5 — Gestion des mises à jour

La gestion des correctifs est un domaine critique : selon l'ANSSI, plus de 70 % des compromissions exploitent des vulnérabilités pour lesquelles un correctif était disponible depuis plus de 30 jours. Ce domaine est particulièrement surveillé lors des audits AirCyber.

- [ ] **Mesure 5.1** — Définir une **politique de gestion des correctifs** formalisée avec des délais cibles : critique ≤ 72h, important ≤ 30 jours, standard ≤ 90 jours
- [ ] **Mesure 5.2** — Appliquer cette politique à tous les composants : systèmes d'exploitation, applications, firmwares, équipements réseau
- [ ] **Mesure 5.3** — Identifier et documenter tous les systèmes en fin de support (*EOL*), avec un plan de migration ou de mitigations compensatoires
- [ ] **Mesure 5.4** — Tester les mises à jour critiques dans un environnement de préproduction avant déploiement en production (si applicable)

## Domaine 6 — Sauvegarde et continuité d'activité

Les **ransomwares** sont la menace numéro un pour les PME industrielles. La stratégie de sauvegarde *3-2-1* (3 copies, 2 supports différents, 1 hors site) est le minimum requis pour résister à une attaque et reprendre l'activité rapidement.

- ☐ **Mesure 6.1** — Mettre en place des sauvegardes automatiques, chiffrées, avec au moins une copie **hors ligne** (déconnectée du réseau) pour résister aux ransomwares
- ☐ **Mesure 6.2** — Tester les restaurations au moins une fois par an et documenter les résultats (rapport de test avec RTO/RPO constatés)
- ☐ **Mesure 6.3** — Rédiger un **Plan de Reprise d'Activité (PRA)** définissant les priorités de reprise, les RTO et RPO cibles, et les responsabilités
- ☐ **Mesure 6.4** — Couvrir par les sauvegardes toutes les données critiques : données métier, données de conception (CAO/FAO), données contractuelles

## Domaine 7 — Journalisation et surveillance

La *journalisation* permet de détecter les incidents, de comprendre les attaques a posteriori et de fournir des preuves forensiques en cas d'enquête. C'est aussi un prérequis pour répondre aux exigences des donneurs d'ordres en cas d'incident affectant leur supply chain.

- ☐ **Mesure 7.1** — Activer et centraliser la **journalisation** sur tous les équipements critiques : serveurs, pare-feu, équipements réseau, annuaire Active Directory
- ☐ **Mesure 7.2** — Conserver les journaux au minimum 1 an pour les équipements critiques, en garantissant leur intégrité (journaux non modifiables)

- [ ] **Mesure 7.3** — Mettre en place des alertes sur les événements suspects : tentatives de connexion échouées répétées, accès en dehors des heures ouvrées, volume anormal de données transférées

- [ ] **Mesure 7.4** — Synchroniser les horloges de tous les équipements sur un serveur NTP fiable (indispensable pour corréler les événements lors d'une investigation)

## Domaine 8 — Sensibilisation et formation du personnel

Le facteur humain reste la principale cause de compromission dans les PME. Une politique de sensibilisation efficace réduit significativement le risque de phishing, d'ingénierie sociale et d'erreurs de manipulation. Ce domaine est évalué à la fois sur les supports de formation et sur les comportements observés lors de l'audit.

- [ ] **Mesure 8.1** — Organiser une **formation annuelle obligatoire** de l'ensemble du personnel aux bonnes pratiques de sécurité, avec listes de présence

- [ ] **Mesure 8.2** — Réaliser des exercices de *phishing simulé* au moins une fois par an et analyser les résultats pour adapter la formation

- [ ] **Mesure 8.3** — Afficher des procédures claires pour signaler un incident ou une suspicion de compromission (qui contacter, comment, dans quel délai)

- [ ] **Mesure 8.4** — Former spécifiquement les équipes techniques et dirigeants aux risques spécifiques à l'aéronautique : espionnage industriel, données ITAR, ingénierie sociale ciblée

## Comment utiliser cette checklist

Cette checklist est un outil de **pré-audit interne**, à utiliser avant la visite de l'assesseur accrédité. Pour chaque mesure, notez votre statut actuel : conforme (C), partiellement conforme (PC) ou non conforme (NC). Les mesures NC prioritaires doivent figurer dans votre plan de remédiation.

Accompagnez chaque mesure d'une référence au document probatoire correspondant (voir la liste des documents à préparer pour l'audit AirCyber). L'assesseur s'appuiera sur ces documents pour valider la conformité effective et non seulement déclarative.

Pour une démarche complète, consultez notre guide d'obtention de la labellisation AirCyber Bronze et notre centre de ressources AirCyber. Notre équipe propose un accompagnement AirCyber incluant une pré-évaluation basée sur cette checklist pour identifier rapidement les points de blocage.

Pour les PME soumises à l'exigence Safran, consultez également notre article sur l'obligation AirCyber Bronze chez Safran.

## FAQ — Checklist AirCyber Bronze

### Faut-il être conforme à 100 % des 44 mesures pour obtenir le label Bronze ?

Non. AirCyber Bronze accepte un niveau de conformité partielle sur certaines mesures, à condition que les écarts soient documentés dans un plan d'actions formalisé et que les mesures critiques soient satisfaites. L'assesseur évalue la maturité globale et la trajectoire de mise en conformité, pas uniquement un score binaire.

### Cette checklist couvre-t-elle aussi les mesures sectorielles aéronautiques ?

Cette checklist couvre les 44 mesures ANSSI communes à tous les secteurs. Les mesures sectorielles aéronautiques spécifiques à AirCyber (protection ITAR/EAR, gestion des accès aux

systèmes de conception, traçabilité des modifications sur les données techniques) sont évaluées séparément par l'assesseur et ne font pas partie du Guide d'Hygiène Informatique de l'ANSSI publié.

### Puis-je utiliser cette checklist pour préparer une certification ISO 27001 ?

Partiellement. Les 44 mesures ANSSI couvrent une large portion des contrôles de l'ISO 27001:2022, notamment les annexes A relatives à la sécurité physique, aux accès logiques et à la gestion des actifs. Cependant, l'ISO 27001 exige en plus un *SMSI* complet avec gestion des risques formalisée, revues de direction et audit interne — des éléments absents du référentiel Bronze. Vous trouverez plus d'informations dans notre guide sur l'AirCyber Silver, qui s'aligne sur la couverture ISO 27001.



## Pour aller plus loin : Mise en œuvre pratique

La conformité réglementaire nécessite une approche structurée et documentée. Ces ressources complémentaires permettent d'approfondir les points techniques et juridiques abordés dans cet article.

### Outils d'auto-évaluation

**ANSSI — Outil d'évaluation cybersécurité** — Le Diagnostic de Cybersécurité de l'ANSSI permet d'évaluer le niveau de maturité de votre organisation sur 5 domaines clés. Gratuit et disponible sur diagnostic.ssi.gouv.fr.

**ENISA — Outil d'auto-évaluation NIS2** — Questionnaire structuré pour identifier les exigences applicables à votre secteur et votre taille d'organisation.

**Logiciels GRC** — Des solutions comme Vanta, Drata ou TrustCloud automatisent la collecte de preuves de conformité et accélèrent les processus d'audit.

### Documentation à produire en priorité

Politique de Sécurité du Système d'Information (PSSI) — document fondateur

Registre des activités de traitement (RGPD, article 30)

Analyse d'impact relative à la protection des données (AIPD/DPIA)

Plan de continuité d'activité (PCA) et plan de reprise d'activité (PRA)

Procédure de gestion des incidents de sécurité (notification ANSSI/CNIL)

### Accompagnement et conseil

La mise en conformité implique souvent une assistance externe pour les organisations ne disposant pas d'expertise interne. Les RSSI externalisés ou les consultants spécialisés en conformité peuvent accélérer significativement le processus, notamment pour la préparation aux audits de certification ISO 27001 ou pour la mise en conformité NIS 2 avec un délai contraint.

## 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.

## Bonnes pratiques et recommandations complémentaires

Au-delà des techniques et outils présentés dans cet article, plusieurs principes transverses guident les professionnels de la cybersécurité dans leur approche quotidienne. La défense en profondeur (*defense-in-depth*) reste le principe fondateur : aucune mesure de sécurité unique n'est suffisante, et la multiplication des couches de protection — même imparfaites individuellement — crée une résilience globale supérieure à la somme de ses parties.

### Veille et mise à jour continue

La cybersécurité est un domaine où l'obsolescence est rapide. Une technique ou un outil efficace en 2024 peut être contourné en 2026. Les équipes sécurité maintiennent leur efficacité en s'appuyant sur des sources de veille fiables : bulletins CERT-FR et ANSSI, advisories des éditeurs (Microsoft MSRC, Google Project Zero, Cisco Talos), recherches académiques (USENIX Security, IEEE S&P, CCS), et publications de la communauté (threat intel reports des grands éditeurs, articles de blog de chercheurs reconnus).

### Documentation et partage de connaissances

La capitalisation des connaissances est un enjeu organisationnel critique dans les équipes de sécurité. Les runbooks d'investigation, les post-mortems d'incidents, les procédures de réponse documentées, et les bases de connaissance internes permettent de maintenir la cohérence des pratiques indépendamment des rotations d'équipe et de réduire le temps de résolution des incidents récurrents. L'utilisation d'un wiki sécurisé (Confluence, Notion avec contrôles d'accès stricts) pour centraliser ces connaissances est une pratique adoptée par la majorité des équipes SOC matures. La documentation proactive, rédigée juste après les incidents pendant que les détails sont frais, est systématiquement plus précise et utile que la documentation rédigée après coup.

## 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.