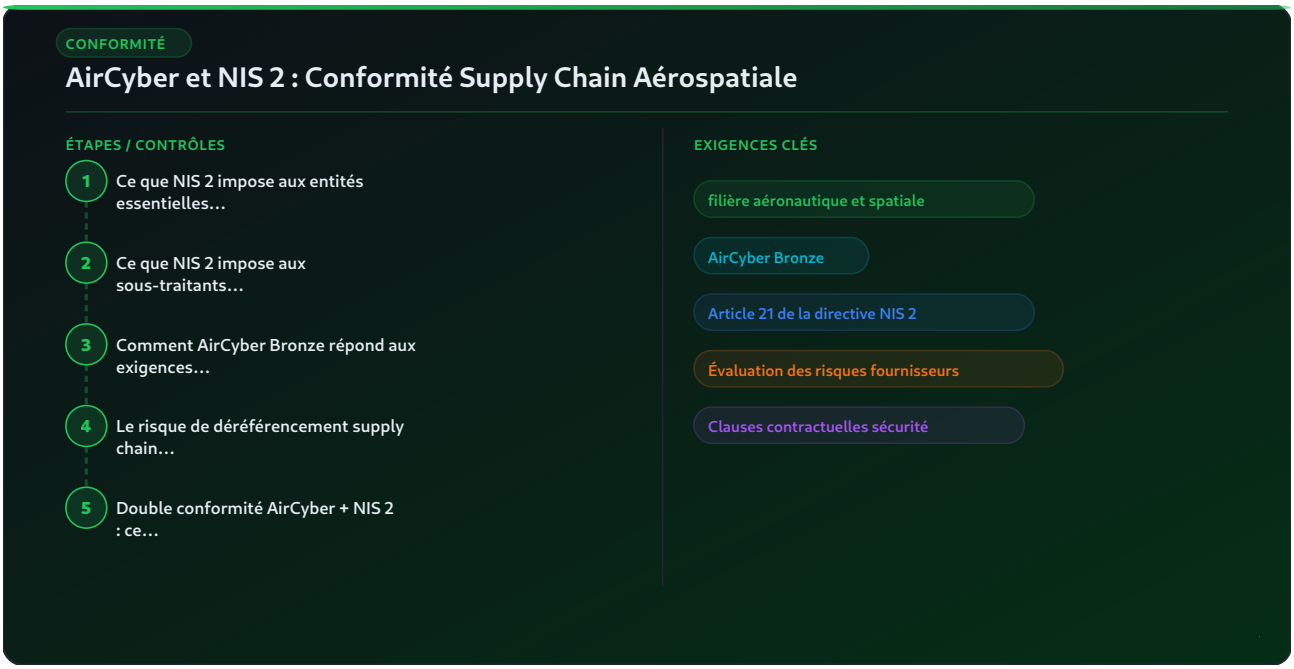
AirCyber et NIS 2 : Conformité Supply Chain Aérospatiale

> NIS 2 oblige Airbus, Dassault, Safran à sécuriser leur supply chain. Comment AirCyber Bronze répond aux exigences NIS 2 pour les sous-traitants…

La directive **NIS 2** (Network and Information Security 2), transposée en droit français fin 2024 et dont les obligations entrent pleinement en application pour les sous-traitants à partir de fin 2027, crée un mécanisme de cascade réglementaire inédit dans la **filière aéronautique et spatiale**. Les *entités essentielles* comme Airbus, Dassault Aviation, Safran et Thales — membres fondateurs de BoostAerospace depuis 2011 — sont directement assujetties à NIS 2 et doivent désormais démontrer qu'elles sécurisent l'ensemble de leur chaîne d'approvisionnement numérique. Cette obligation de cascade impose aux sous-traitants et équipementiers de démontrer leur maturité cybersécurité sous peine de déréférencement commercial. Dans ce contexte, le label **AirCyber Bronze**, avec ses 44 mesures ANSSI et ses exigences sectorielles, s'impose comme la réponse la plus naturelle et la plus rapide pour les sous-traitants aérospatiaux cherchant à satisfaire simultanément les exigences de leurs donneurs d'ordre et la réglementation NIS 2. Ce dossier analyse point par point les synergies et complémentarités entre les deux référentiels.



Ce que NIS 2 impose aux entités essentielles aérospatiales

L'**Article 21 de la directive NIS 2** impose aux entités essentielles un ensemble de mesures de gestion des risques de cybersécurité qui s'étendent explicitement à la *chaîne d'approvisionnement*. Pour les grands donneurs d'ordre aérospatiaux, cela se traduit concrètement par :

Évaluation des risques fournisseurs : obligation d'analyser les risques cyber introduits par chaque prestataire et sous-traitant ayant accès au SI

Clauses contractuelles sécurité : intégration d'exigences minimales de cybersécurité dans tous les contrats de sous-traitance

Surveillance continue : mécanismes de vérification périodique de la conformité des sous-traitants

Notification d'incidents : obligation de remontée d'information en cas d'incident affectant la chaîne d'approvisionnement

Pénalités : amendes pouvant atteindre **10 M€ ou 2% du CA mondial** pour les entités essentielles en cas de non-conformité

Ces obligations transforment fondamentalement la relation donneur d'ordre / sous-traitant : un équipementier sans preuve de maturité cyber devient un risque légal direct pour son client.

Ce que NIS 2 impose aux sous-traitants aérospatiaux

Si les sous-traitants ne sont pas directement soumis à NIS 2 (sauf s'ils dépassent les seuils d'entité importante), ils subissent la pression contractuelle de leurs clients. Concrètement, les sous-traitants auront à :

> ⚡ **Retour terrain**
>
> J'ai réalisé un audit de conformité PCI-DSS pour un e-commerçant de taille moyenne. La surprise : leur prestataire de paiement gérait effectivement la conformité PCI côté serveur, mais les formulaires de carte côté client passaient par leurs propres serveurs via un JavaScript personnalisé — introduisant un scope PCI non déclaré. La remédiation a nécessité une migration vers un formulaire de paiement hébergé (redirect ou iFrame).

Démontrer leur niveau de maturité cyber via une **labellisation reconnue** (AirCyber, ISO 27001) ou un questionnaire d'évaluation

Mettre en place des **procédures de notification d'incidents** vers leurs donneurs d'ordre dans des délais contraints (72h)

Appliquer des mesures de sécurité minimales sur les actifs traitant des **données ou des systèmes du donneur d'ordre**

Documenter leur **politique de gestion des risques cyber** liés à la chaîne d'approvisionnement

Comment AirCyber Bronze répond aux exigences NIS 2 pour les sous-traitants

L'alignement entre AirCyber Bronze et les exigences NIS 2 Article 21 est remarquable. Les **44 mesures de Bronze couvrent les principaux domaines NIS 2** applicables aux sous-traitants :

Exigence NIS 2 Art. 21	Couverture AirCyber Bronze
Gestion des risques cyber	✓ Analyse de risques simplifiée obligatoire
Politique de sécurité	✓ PSSI obligatoire, validée par direction
Gestion des incidents	✓ Procédure de gestion des incidents requise
Continuité des activités	✓ PCA/PRA simplifié exigé
Sécurité des réseaux	✓ Cloisonnement réseau, pare-feu, VPN
Contrôles d'accès	✓ Gestion des comptes, MFA, annuaire
Chiffrement	✓ Chiffrement des données sensibles requis
Sensibilisation du personnel	✓ Formation annuelle obligatoire, charte SI

AirCyber Bronze ne couvre pas exhaustivement NIS 2 (notamment les aspects de gouvernance avancée et les obligations de reporting direct vers l'ANSSI), mais il constitue une base solide et sectorielle reconnue qui répond à l'essentiel des attentes contractuelles des donneurs d'ordre assujettis à NIS 2.

Le risque de déréférencement supply chain pour les non-conformes

Le risque pour les sous-traitants non-conformes est concret et croissant. Les pénalités NIS 2 en France entrent pleinement en vigueur fin 2027 pour la chaîne d'approvisionnement, mais les donneurs d'ordre n'attendent pas cette échéance : **les clauses contractuelles cyber sont déjà intégrées dans les nouveaux appels d'offres Airbus, Dassault et Safran**.

Un sous-traitant sans labellisation AirCyber expose son donneur d'ordre à un risque de non-conformité NIS 2, ce qui peut conduire à :

Une **suspension ou résiliation de contrat** lors du renouvellement

Un **déclassement dans la qualification fournisseur** (impact sur les volumes alloués)

Une **exclusion des appels d'offres futurs** nécessitant un niveau de maturité démontré

La **perte de statut de fournisseur qualifié** pour les programmes sensibles

---

Double conformité AirCyber + NIS 2 : ce qu'il faut faire en plus

Pour les entreprises directement assujetties à NIS 2 (entités importantes dépassant 50 salariés ou 10 M€ de CA dans un secteur critique), AirCyber Bronze ne suffit pas seul. La double conformité exige des compléments :

Enregistrement auprès de l'ANSSI via le portail MonEspaceNIS2 (obligation légale)

Notification d'incidents en 24h/72h/30j selon le niveau de gravité

Désignation d'un point de contact NIS 2 identifié auprès des autorités

Extension de l'analyse de risques à l'ensemble de la chaîne d'approvisionnement numérique

Tests de pénétration annuels sur les systèmes critiques (recommandé NIS 2, non obligatoire Bronze)

Notre service d'accompagnement AirCyber intègre ces compléments NIS 2 dans la feuille de route globale. Consultez également notre Centre de Ressources AirCyber pour les modèles documentaires adaptés.

CERT Aviation : rôle dans la détection et l'alerte

Créé en **novembre 2022 par 9 fondateurs** de la filière aéronautique, le *CERT Aviation* (Computer Emergency Response Team sectoriel) joue un rôle central dans l'articulation entre AirCyber et NIS 2. Ses missions :

Collecte et analyse des incidents remontés par les membres AirCyber

Diffusion d'alertes sectorielles sur les menaces spécifiques à l'aéronautique (ransomware, espionnage industriel)

Coordination avec l'ANSSI pour les incidents majeurs relevant de NIS 2

Partage de renseignement sur les menaces (CTI) entre membres du réseau

Reconnaissance mondiale comme **Aviation ISAC** lors du sommet de Dublin en 2023

À RETENIR

Points clés à retenir

✓ **NIS 2 cascade** : les entités essentielles (Airbus, Dassault, Safran, Thales) doivent sécuriser leurs sous-traitants

✓ **AirCyber Bronze couvre ~80%** des exigences NIS 2 applicables aux sous-traitants

✓ **Risque concret dès 2025** : clauses contractuelles cyber déjà en vigueur chez les grands donneurs d'ordre

✓ **Double conformité** : enregistrement ANSSI + notification incidents si entité importante

✓ **CERT Aviation** = filet de sécurité sectoriel pour la détection et la coordination d'incidents

FAQ : AirCyber et NIS 2

Un sous-traitant aéronautique est-il directement soumis à NIS 2 ?

Pas automatiquement. La directive NIS 2 s'applique directement aux entités essentielles et importantes selon des critères de taille (50+ salariés ou 10 M€+ de CA) et de secteur. Cependant, même les PME non-assujetties directement subissent la pression contractuelle de leurs clients donneurs d'ordre assujettis, qui doivent sécuriser leur chaîne d'approvisionnement pour respecter leurs propres obligations NIS 2.

AirCyber Bronze suffit-il pour satisfaire les clauses NIS 2 imposées par Airbus ou Dassault ?

Dans la grande majorité des cas, oui. Les clauses contractuelles dérivées de NIS 2 que les donneurs d'ordre intègrent dans leurs appels d'offres référencent des niveaux de maturité compatibles avec AirCyber Bronze. Certains contrats très sensibles peuvent exiger Silver ou un audit spécifique — vérifiez toujours les clauses exactes de votre contrat.

Quelle est la différence entre AirCyber et NIS 2 en termes d'obligations de notification ?

AirCyber Bronze prévoit une procédure de gestion des incidents interne et une remontée vers le CERT Aviation pour les incidents significatifs. NIS 2 impose en plus une notification obligatoire à l'ANSSI en 24h (alerte préliminaire), 72h (notification complète) et 30 jours (rapport final) pour les entités assujetties. Ces obligations de notification sont complémentaires et non redondantes.

Articles complémentaires

→ Guide complet : obtenir la labellisation AirCyber Bronze

→ AirCyber vs ISO 27001 : différences et complémentarité

→ AirCyber Silver : exigences et feuille de route

→ Financement AirCyber : subventions et aides pour PME

Double conformité AirCyber + NIS 2 ?

Nos experts vous accompagnent pour construire une feuille de route qui satisfait simultanément les exigences AirCyber et NIS 2, sans doublon ni lacune.

Évaluer ma conformité →

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.

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.

