AERO EXCELLENCE™ V2 GIFAS : Guide Complet pour les Sous-traitants Aéronautiques

AERO EXCELLENCE™ V2 est le référentiel de labellisation cybersécurité édité par le GIFAS (Groupement des Industries Françaises Aéronautiques et Spatiales) pour l'ensemble de la supply chain aéronautique française. Déployé à grande échelle depuis 2023 et mis à jour en version 2 pour répondre aux nouvelles menaces cyber ciblant le secteur, ce label constitue aujourd'hui un prérequis contractuel pour de nombreux sous-traitants travaillant avec Airbus, Safran, Dassault Aviation, Thales, ATR ou MBDA. Comprendre son fonctionnement, ses trois niveaux d'exigence et son articulation avec d'autres dispositifs comme AirCyber BoostAerospace est devenu une nécessité stratégique pour les PME et ETI de la filière. Ce guide complet couvre l'historique du GIFAS et de sa démarche de labellisation, les évolutions majeures de la V2 par rapport à la V1, le détail des niveaux Bronze, Silver et Gold, le processus concret d'obtention du label, les coûts et délais réalistes, ainsi que les synergies avec les autres dispositifs de cybersécurité sectorielle afin que chaque sous-traitant puisse construire une feuille de route adaptée à son contexte et à ses donneurs d'ordre.

Le GIFAS et la naissance d'AERO EXCELLENCE™

Le Groupement des Industries Françaises Aéronautiques et Spatiales regroupe plus de 430 entreprises représentant l'ensemble du tissu industriel aéronautique, spatial et de défense en France. Fondé en 1908, le GIFAS est l'interlocuteur privilégié des pouvoirs publics, de l'ANSSI et des institutions européennes pour toutes les questions touchant à la souveraineté industrielle du secteur. Face à la recrudescence des cyberattaques ciblant la supply chain aéronautique — notamment les campagnes APT attribuées à des acteurs étatiques cherchant à exfiltrer des données techniques sensibles — le GIFAS a décidé en 2019 de structurer une démarche

commune de montée en maturité cybersécurité pour l'ensemble de ses membres et de leurs sous-traitants.

Le premier référentiel AERO EXCELLENCE™ V1 a été publié en 2020. Il s'inspirait fortement des meilleures pratiques issues de l'ISO 27001, du NIST Cybersecurity Framework et du référentiel Prestataires de Services Essentiels (PSE) de l'ANSSI, mais dans une version allégée et pragmatique adaptée aux PME industrielles qui ne disposent pas toujours d'une DSI dédiée. La V1 proposait deux niveaux de labellisation et une centaine de contrôles organisés autour des thématiques gouvernance, technique, physique et documentaire.

Suite aux retours terrain des premiers labels délivrés et à l'évolution du paysage des menaces, le GIFAS a entamé la refonte du référentiel dès 2022, aboutissant à la publication d'AERO EXCELLENCE™ V2 en 2023. Cette nouvelle version introduit un troisième niveau (Gold), renforce les exigences techniques sur la gestion des identités, le cloisonnement réseau et la détection d'incidents, et précise les modalités d'audit par des organismes tiers accrédités.

AERO EXCELLENCE™ V2 vs V1 : les évolutions majeures

La version 2 du référentiel GIFAS représente une évolution substantielle, tant sur le fond que sur la forme. Voici les principales différences que les sous-traitants ayant déjà obtenu un label V1 doivent connaître :

Structure à trois niveaux au lieu de deux

La V1 proposait un niveau de base (équivalent au Bronze actuel) et un niveau avancé. La V2 introduit trois paliers distincts — Bronze, Silver et Gold — permettant une progression graduée et une reconnaissance plus fine du niveau de maturité atteint. Cette granularité supplémentaire est particulièrement utile pour les PME qui peuvent commencer par le Bronze, démontrer leur engagement et progresser vers Silver ou Gold selon les exigences contractuelles de leurs clients.

Intégration des exigences NIS 2

La V2 anticipe l'entrée en application de la directive NIS 2 transposée en droit français. Les contrôles du niveau Silver et Gold sont alignés sur les obligations imposées aux entités importantes et essentielles dans le secteur aéronautique, facilitant ainsi la double conformité pour les sous-traitants concernés par NIS 2.

Renforcement des exigences sur la chaîne d'approvisionnement logicielle

La V2 introduit des contrôles spécifiques sur la gestion des composants logiciels tiers (SBOM — Software Bill of Materials), la sécurité des outils de développement et la vérification de l'intégrité des mises à jour logicielles. Ces contrôles sont obligatoires dès le niveau Silver et reflètent les leçons tirées des incidents SolarWinds et Kaseya qui ont touché des industriels du secteur.

Exigences documentaires renforcées

La V1 acceptait des politiques de sécurité peu formalisées. La V2 exige des documents structurés, révisés annuellement et approuvés par la direction, conformément aux bonnes pratiques ISO 27001. Un plan de traitement des risques formalisé est requis dès le niveau Bronze.

Audit par tiers accrédité obligatoire à partir du Silver

En V1, l'auto-évaluation était davantage acceptée. En V2, le niveau Silver et Gold nécessitent un audit par un organisme de vérification tiers accrédité par le GIFAS, ce qui renforce la crédibilité du label aux yeux des donneurs d'ordre mais implique des coûts supplémentaires.

Les trois niveaux de labellisation : Bronze, Silver, Gold

Niveau Bronze — La fondation cybersécurité

Le niveau Bronze constitue le point d'entrée dans la labellisation AERO EXCELLENCE™ V2. Il cible les entreprises de la supply chain qui traitent des données peu sensibles mais souhaitent démontrer leur engagement dans une démarche structurée de cybersécurité. Le référentiel Bronze comprend environ 60 contrôles répartis sur 8 domaines :

Gouvernance : existence d'une politique de sécurité approuvée par la direction, nomination d'un référent sécurité (qui peut cumuler ce rôle avec d'autres fonctions dans les PME), réalisation d'une analyse de risques simplifiée, sensibilisation annuelle des collaborateurs.

Gestion des accès : mise en place d'une politique de mots de passe robuste (longueur minimale, complexité, renouvellement), gestion des comptes privilégiés, suppression des comptes des collaborateurs quittant l'entreprise dans des délais définis.

Protection des postes de travail : déploiement d'un antivirus/EDR sur l'ensemble des postes, chiffrement des disques durs, gestion des mises à jour de sécurité sous 30 jours.

Sécurité réseau : segmentation basique entre réseau bureautique et réseau de production, firewall correctement configuré, audit des flux autorisés.

Sauvegarde et continuité : politique de sauvegarde des données critiques, tests de restauration réguliers, procédure de continuité documentée.

Gestion des incidents : procédure de signalement des incidents, log des événements de sécurité, point de contact GIFAS en cas d'incident majeur.

Le niveau Bronze est accessible en auto-évaluation guidée, complétée par une vérification documentaire par le GIFAS ou un partenaire agréé. Les délais typiques d'obtention sont de 3 à 4 mois pour une entreprise qui part de zéro, ou 6 à 8 semaines pour une entreprise ayant déjà des bases en cybersécurité.

Niveau Silver — La maturité opérationnelle

Le niveau Silver s'adresse aux sous-traitants traitant des données techniques sensibles, des informations à diffusion restreinte ou des données ITAR/EAR, ainsi qu'aux entreprises souhaitant répondre aux appels d'offres d'un plus grand nombre de donneurs d'ordre. Avec environ 120 contrôles, il va significativement plus loin que le Bronze sur plusieurs dimensions :

Gestion avancée des identités : authentification multi-facteurs (MFA) pour tous les accès distants et les comptes administrateurs, revue trimestrielle des droits d'accès, gestion des comptes de service.

Détection et réponse aux incidents : déploiement d'un SIEM ou d'une solution de détection centralisée, définition de cas d'usage de détection adaptés au contexte industriel, processus de réponse à incident documenté et testé.

Sécurité des développements : si l'entreprise développe des logiciels embarqués ou des outils internes, application d'un cycle de développement sécurisé (SDLC), revues de code, tests de sécurité.

Chiffrement et protection des données : chiffrement des échanges avec les donneurs d'ordre (e-mail sécurisé, VPN avec chiffrement fort), chiffrement des données sensibles au repos.

Sécurité physique renforcée : contrôle d'accès aux locaux techniques, surveillance des entrées/sorties des médias amovibles, politique BYOD.

Le Silver nécessite obligatoirement un audit par un organisme tiers accrédité GIFAS. Les délais typiques d'obtention sont de 6 à 8 mois, en incluant la phase de mise en conformité préalable.

Niveau Gold — L'excellence en cybersécurité

Le niveau Gold est destiné aux sous-traitants stratégiques qui traitent des données hautement sensibles (secrets de fabrication, données de défense, propriété intellectuelle critique) ou qui ont un accès direct aux systèmes d'information des donneurs d'ordre. Avec plus de 180 contrôles, il approche le niveau d'exigence d'une certification ISO 27001 :

SOC interne ou externalisé : surveillance continue de la sécurité 24h/24, capacité de détection et de réponse en temps réel, exercices de simulation d'attaque (red team) annuels.

Gestion avancée des tiers : évaluation cybersécurité de tous les sous-traitants critiques, clauses contractuelles cybersécurité, audits réguliers des fournisseurs stratégiques.

Résilience avancée : PCA/PRA testé annuellement, capacité de reprise d'activité sous 4 heures pour les fonctions critiques, exercices de crise cyber.

Intelligence des menaces : abonnement à des flux CTI (Cyber Threat Intelligence) sectoriels, veille sur les vulnérabilités des équipements industriels utilisés.

Le Gold implique un audit approfondi sur site par un auditeur certifié. Les délais typiques sont de 10 à 12 mois, parfois plus pour les grandes structures. La revalidation est requise tous les 3 ans, avec une surveillance annuelle.

Qui est concerné par AERO EXCELLENCE™ V2 ?

Le label s'adresse à toutes les entreprises de la supply chain aéronautique française, qu'elles soient membres directs du GIFAS ou fournisseurs de rang 2 et 3. En pratique, les donneurs d'ordre suivants l'exigent ou le préconisent fortement dans leurs questionnaires de qualification fournisseurs :

Airbus : impose AERO EXCELLENCE™ V2 Bronze minimum pour tous les nouveaux fournisseurs qualifiés depuis 2024, Silver pour les accès aux systèmes d'information Airbus, Gold pour les sous-traitants ayant accès à des données de classification "Airbus Confidential" ou supérieure.

Safran : intègre AERO EXCELLENCE™ V2 dans son programme "Safran Security By Design" et l'exige de ses sous-traitants critiques définis par un scoring interne. Le niveau exigé dépend de la criticité des données échangées et de la nature des prestations.

Dassault Aviation : applique ses propres exigences en matière de cybersécurité (fortement influencées par les contraintes ITAR/EAR pour les programmes de défense), qui sont compatibles avec AERO EXCELLENCE™ V2. Un sous-traitant Gold est généralement considéré comme répondant aux exigences Dassault.

ATR : coentreprise Airbus/Leonardo, applique les exigences Airbus pour sa supply chain.

Thales : dispose de son propre référentiel cybersécurité fournisseurs, mais AERO EXCELLENCE™ V2 Silver est reconnu comme équivalent pour les programmes civils. Les programmes de défense relèvent d'exigences spécifiques.

MBDA : les exigences ITAR et les contraintes de sécurité défense prévalent, mais AERO EXCELLENCE™ V2 Gold est un point de départ reconnu.

Processus de labellisation étape par étape

Obtenir le label AERO EXCELLENCE™ V2 suit un processus structuré en plusieurs phases :

Étape 1 — Auto-diagnostic initial : Le GIFAS met à disposition un outil d'auto-diagnostic en ligne permettant à l'entreprise d'évaluer son niveau de maturité actuel face aux contrôles du niveau visé. Cette étape, gratuite, prend 2 à 4 heures et produit un rapport de gaps priorisé.

Étape 2 — Plan de remédiation : Sur la base du rapport de gaps, l'entreprise élabore un plan de mise en conformité avec des jalons et des responsables désignés. Pour le niveau Bronze, ce plan peut être réalisé en interne. Pour Silver et Gold, il est recommandé de faire appel à un conseil spécialisé.

Étape 3 — Mise en conformité : Déploiement des mesures techniques et organisationnelles identifiées dans le plan de remédiation. Cette phase est la plus longue et la plus coûteuse, représentant l'essentiel du budget.

Étape 4 — Audit de labellisation : Pour le Bronze, remise du dossier documentaire à un organisme de vérification agréé. Pour Silver et Gold, audit sur site incluant des tests techniques (scans de vulnérabilités, revue de configuration, entretiens avec les équipes).

Étape 5 — Décision de labellisation : L'organisme de vérification transmet son rapport au GIFAS, qui prend la décision finale de labellisation. En cas d'écarts mineurs, un plan d'action correctif sous 3 mois peut être accepté.

Étape 6 — Maintien du label : Le label est valable 3 ans, avec une surveillance annuelle (bilan documentaire et vérification des indicateurs clés). Tout incident de sécurité majeur doit être signalé au GIFAS dans les 72 heures.

Coûts et délais typiques

Les coûts d'obtention d'AERO EXCELLENCE™ V2 varient considérablement selon la taille de l'entreprise, son niveau de maturité initial et le niveau visé. Voici des ordres de grandeur représentatifs pour une PME de 50 à 200 salariés :

Niveau Bronze : La mise en conformité représente généralement entre 15 000 € et 40 000 € en coûts directs (solutions techniques + prestations conseil + frais d'audit), auxquels s'ajoutent les coûts internes (temps passé). Les délais d'obtention sont de 3 à 6 mois selon le point de départ.

Niveau Silver : Entre 40 000 € et 100 000 € en coûts directs, principalement liés au déploiement d'outils de détection (SIEM, EDR avancé), à l'implémentation de l'authentification multi-facteurs et aux prestations de conseil spécialisé. Délais : 6 à 12 mois.

Niveau Gold : Au-delà de 100 000 € en coûts directs, souvent entre 150 000 € et 300 000 € selon la complexité du SI et la nécessité ou non d'externaliser le SOC. Délais : 12 à 18 mois.

Des aides financières existent : le dispositif Cyber PME de l'ANSSI, les aides régionales à la transformation numérique et, dans certains cas, des participations des donneurs d'ordre eux-mêmes dans le cadre de programmes de soutien à la supply chain.

Articulation avec AirCyber BoostAerospace

AirCyber est le programme de cybersécurité développé par BoostAerospace (filiale d'Airbus, Dassault Aviation, Safran et Thales) pour sécuriser les échanges de données dans la supply chain. Contrairement à AERO EXCELLENCE™ V2 qui est un référentiel de labellisation général de la filière GIFAS, AirCyber se concentre sur la sécurisation des accès aux plateformes collaborative de partage de données (notamment AirSupply et MyAirbus).

Les deux dispositifs sont complémentaires et non redondants : AERO EXCELLENCE™ V2 atteste du niveau de maturité global de l'organisation, tandis qu'AirCyber garantit la sécurité des échanges de données avec les donneurs d'ordre partenaires de BoostAerospace. Un sous-traitant Airbus aura typiquement besoin des deux : AERO EXCELLENCE™ V2 Bronze ou Silver pour

sa qualification fournisseur générale, et la certification AirCyber pour accéder aux portails collaboratifs Airbus.

La bonne nouvelle est que les contrôles d'AERO EXCELLENCE™ V2 Silver couvrent en grande partie les exigences AirCyber, ce qui limite le surcoût de double conformité. Un sous-traitant Silver AERO EXCELLENCE™ V2 qui engage une démarche AirCyber n'aura généralement que des efforts marginaux à fournir sur la partie AirCyber.

À RETENIR

À retenir

AERO EXCELLENCE™ V2 est le référentiel cybersécurité du GIFAS, avec trois niveaux Bronze (60 contrôles), Silver (120 contrôles) et Gold (180+ contrôles) adaptés à la progressivité de la supply chain aéronautique.

La V2 apporte des évolutions majeures par rapport à la V1 : troisième niveau Gold, alignement NIS 2, exigences SBOM, audit tiers obligatoire dès le Silver.

Les principaux donneurs d'ordre (Airbus, Safran, Dassault, Thales, ATR) intègrent AERO EXCELLENCE™ V2 dans leurs critères de qualification fournisseurs depuis 2023-2024.

Les coûts d'obtention vont de 15 000 € à 300 000 € selon le niveau visé et la maturité initiale, avec des délais de 3 à 18 mois.

AERO EXCELLENCE™ V2 et AirCyber sont complémentaires : le premier atteste de la maturité globale, le second sécurise les accès aux plateformes collaboratives BoostAerospace.

FAQ sur AERO EXCELLENCE™ V2 GIFAS

Quelle est la différence entre AERO EXCELLENCE™ V1 et V2 ?

La V2 introduit un troisième niveau de labellisation (Gold), renforce les exigences techniques sur la détection d'incidents, la gestion des identités et la sécurité de la chaîne logicielle, et rend obligatoire l'audit par tiers accrédité dès le niveau Silver. La V1 était plus permissive sur l'auto-évaluation et ne comportait que deux niveaux.

AERO EXCELLENCE™ V2 Bronze est-il suffisant pour travailler avec Airbus ?

Le Bronze est le niveau minimal exigé pour les nouveaux fournisseurs Airbus depuis 2024. Cependant, selon la nature des données échangées et le type d'accès aux systèmes Airbus, le Silver voire le Gold peuvent être requis. Il est recommandé de consulter directement son interlocuteur Airbus pour connaître le niveau applicable à sa situation contractuelle.

Combien de temps est valable le label AERO EXCELLENCE™ V2 ?

Le label est valable 3 ans à compter de la date de délivrance, sous réserve de la surveillance annuelle et du signalement de tout incident majeur. À l'issue des 3 ans, un audit de renouvellement est nécessaire pour maintenir la labellisation.

Peut-on faire une demande de label AERO EXCELLENCE™ V2 sans être membre du GIFAS ?

Oui. Le label est accessible à toutes les entreprises de la supply chain aéronautique, qu'elles soient ou non membres du GIFAS. Les entreprises non membres peuvent néanmoins avoir un processus d'accès légèrement différent — il est recommandé de contacter directement le GIFAS pour connaître les modalités applicables.

Comment se préparer efficacement à l'audit de labellisation ?

La préparation passe par trois étapes clés : réaliser l'auto-diagnostic GIFAS pour identifier les gaps, mettre en œuvre un plan de remédiation priorisé par criticité et par délai, et simuler l'audit en interne (ou avec un conseil externe) avant la date officielle. Un pré-audit réalisé 4 à 6 semaines avant l'audit officiel permet d'identifier les derniers points de non-conformité à corriger.

AERO EXCELLENCE™ V2 et la transformation numérique aéronautique

La montée en puissance d'AERO EXCELLENCE™ V2 s'inscrit dans un contexte plus large de transformation numérique de la filière aéronautique. Les usines du futur, l'impression 3D de pièces certifiées, la co-conception en temps réel via des jumeaux numériques et le déploiement de l'intelligence artificielle dans les processus de contrôle qualité génèrent de nouveaux flux de données sensibles qui élargissent considérablement la surface d'attaque des sous-traitants. Un fondeur qui imprime des pièces de turbine selon des modèles 3D Safran ou un assembleur qui reçoit des plans numériques signés électroniquement par Airbus traite désormais des actifs numériques d'une valeur stratégique comparable à leurs homologues physiques. AERO EXCELLENCE™ V2 prend en compte cette réalité en intégrant des contrôles spécifiques à la protection des données de fabrication numérique, à la sécurité des outils de CAO/FAO et à la traçabilité des modifications apportées aux fichiers techniques. Les sous-traitants qui anticipent ces exigences et intègrent la cybersécurité dans leur stratégie de transformation numérique — plutôt que de la traiter comme une contrainte réglementaire séparée — bénéficieront d'un avantage compétitif durable dans la supply chain aéronautique de demain.

Pour aller plus loin sur la conformité cybersécurité du secteur aéronautique et les certifications disponibles, consultez nos guides sur AirCyber BoostAerospace et notre page dédiée à AERO EXCELLENCE™ V2. L'ANSSI publie également des guides sectoriels pour accompagner les PME industrielles dans leur démarche de cybersécurité. Le GIFAS met à disposition des ressources complémentaires sur son site gifas.asso.fr. Pour une vision globale de la

réglementation applicable, le portail cyber.gouv.fr centralise l'ensemble des obligations et recommandations des autorités françaises en matière de cybersécurité industrielle.