

Formaliser des exigences de cybersécurité applicables aux produits et services critiques de l'industrie aéronautique et spatiale

RS7741 · RS · Publiée

L'essentiel

Code(s) NSF	326n, 326p
Formacode(s)	31045
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	30/09/2026
Date d'échéance	30/09/2029

Certificateur(s)

AIRBUS OPERATIONS · SIRET : 42091691800048

Résumé de la certification

OBJECTIFS ET CONTEXTE

La certification s'inscrit dans des situations professionnelles propres à l'industrie aéronautique et spatiale, caractérisées par des systèmes critiques, des environnements fortement réglementés et des processus formalisés de validation, de certification et de conformité.

Dans ces contextes, les produits et services (systèmes embarqués, segments sol, infrastructures associées) sont soumis à des référentiels sectoriels spécifiques (notamment DO-326A/ED-202A, PART-IS et exigences des autorités compétentes), imposant la formalisation d'exigences de cybersécurité dérivées d'analyses de risques, traçables, vérifiables et justifiées tout au long du cycle de vie des systèmes, en articulation avec les exigences de sûreté.

Dans ce cadre, les professionnels interviennent, sur un périmètre défini et dans leur périmètre d'intervention, en contribution à des activités d'ingénierie, pour formaliser des exigences de cybersécurité cohérentes avec les risques identifiés et les contraintes applicables.

Leur activité consiste notamment à :

délimiter le périmètre d'analyse cybersécurité en identifiant ses fonctions, ses hypothèses, ses interfaces, ses environnements d'exploitation et les cadres réglementaires applicables;

évaluer les risques de cybersécurité, en prenant en compte les scénarios d'atteinte plausibles et leurs impacts sur les opérations, la sûreté, la disponibilité, l'intégrité et la confidentialité des systèmes et des données ;

formaliser des exigences de cybersécurité vérifiables, traçables et priorisées en termes d'assurance, techniques et organisationnels et de contraintes spécifiques au contexte industriel;

définir des modalités de validation et de vérification associées en précisant les méthodes, les critères et les éléments et type de preuve attendus

préparer et communiquer les exigences de manière argumentée en vue de leur intégration dans des processus formels de validation ou de décision

La certification atteste de la capacité à produire des exigences spécifiées, associées à des méthodes de vérification, des critères d'acceptation et des éléments de preuve, directement exploitables dans des démarches de validation et de démonstration de conformité. Elle correspond à des compétences spécialisées mobilisables en contribution, sans couvrir l'ensemble des activités d'ingénierie système, sans responsabilité d'architecture technique ou d'arbitrage réglementaire, et ne constitue pas une habilitation réglementaire.

COMPÉTENCES ATTESTÉES

Délimiter le périmètre d'analyse cybersécurité du produit ou service critique aéronautique ou spatial en identifiant ses

fonctions impactant la sécurité des systèmes opérationnels et d'information, ses hypothèses (personnes de confiance, domaines de confiance...), ses interfaces organisationnelles et techniques, ses environnements d'exploitation, de maintien en condition opérationnelle (MCO), et de maintien en condition de sécurité (MCS) les cadres réglementaires, normatifs ou contractuels applicables (EASA, FAA, ...), et les process correspondants, incluant la documentation (directives, manuels, ...) en s'appuyant lorsque nécessaire sur les fonctions compétentes (RSSI, service conformité, juridique, ...) pour consolider l'analyse d'applicabilité, afin de cadrer la démarche de définition des exigences de cybersécurité au regard des enjeux de sûreté, de sécurité et des obligations applicables.

Évaluer les risques de cybersécurité susceptibles d'affecter le produit ou service critique aéronautique ou spatial sur le périmètre défini, en analysant les actifs exposés (données, fonctions, systèmes et interfaces), les scénarios d'atteinte plausibles et leurs impacts sur la sécurité, le maintien en conditions opérationnelles (MCO), le maintien en condition de sécurité (MCS), ainsi que sur l'image de l'entreprise en lien avec le produit ou service, les impacts sur la confidentialité, l'intégrité et la disponibilité des données et des services du secteur ainsi que leurs effets sur les enjeux métier afin d'établir les priorités de protection nécessaires à la formalisation d'exigences de cybersécurité adaptées.

Formaliser des exigences de cybersécurité applicables au produit ou service critique aéronautique ou spatial, en traduisant les priorités de protection identifiées en spécifications d'assurance, techniques et organisationnelles, vérifiables et traçables, compatibles avec les contraintes d'architecture, de configuration, d'exploitation, de maintenabilité et de conformité du secteur, afin de permettre leur intégration maîtrisée dans un environnement réglementé sans compromettre l'activité opérationnelle, la sécurité, le maintien en conditions opérationnelles (MCO), le maintien en condition de sécurité (MCS) ainsi que l'image de l'entreprise.

Définir des modalités de validation et de vérification des exigences de cybersécurité du produit ou service critique aéronautique ou spatial, en définissant les méthodes d'évaluation adaptées aux environnements embarqués, industriels ou de services opérationnels, les critères de validation et d'acceptation mesurables et les éléments et types de preuve requis, afin de préparer la démonstration de conformité aux exigences de sécurité applicables.

Présenter de manière argumentée les exigences de cybersécurité du produit ou service critique aéronautique ou spatial auprès des parties prenantes concernées, en démontrant la cohérence entre le contexte analysé, les risques évalués, les exigences formalisées et les modalités de validation et de vérification proposées, en explicitant les conséquences ou implications associées y compris en situation de crise, afin d'éclairer la prise de décision dans le cadre des processus formels de validation en environnement réglementé.

Secteur d'activité et type d'emploi

RÉGLEMENTATIONS D'ACTIVITÉ

Aucune réglementation spécifique ne conditionne l'exercice des activités visées par la certification, cependant elles s'inscrivent dans des environnements industriels fortement réglementés, en particulier dans les secteurs aéronautique et spatial, caractérisés par des exigences élevées en matière de sécurité des opérations, de sûreté et de conformité [1]. Ces cadres imposent l'intégration de la cybersécurité tout au long du cycle de vie des systèmes, ainsi que la production d'éléments documentés permettant d'en démontrer la prise en compte. La certification est directement structuré par ces exigences. Il ne se limite pas à la connaissance des cadres réglementaires, mais vise leur mise en œuvre opérationnelle dans des activités d'ingénierie, en lien avec les processus de certification industrielle. Ainsi, les compétences intègrent de manière opérationnelle les cadres réglementaires et normatifs, permettant d'identifier les exigences de cybersécurité applicables, de les intégrer dans l'analyse de risques, de les formaliser et de préparer la démonstration de conformité. Et leur maîtrise, leur prise en compte et leur respect sont évalués.

[1] Les produits et services concernés (systèmes embarqués, segments sol, infrastructures associées) sont soumis à des cadres réglementaires et normatifs définis par les autorités de certification (notamment EASA, FAA) et par des référentiels sectoriels spécifiques, parmi lesquels on peut citer les principaux cadres de référence : la réglementation PART-IS (Information Security), qui impose aux organisations du secteur aéronautique la mise en place d'un système de gestion de la sécurité de l'information incluant l'identification, l'évaluation et le traitement des risques de cybersécurité ; les normes DO-326A / ED-202A et leurs documents associés (DO-356A / ED-203A, DO-355 / ED-204), qui encadrent la prise en compte de la cybersécurité dans les processus de conception, de développement et de certification des systèmes aéronautiques ; les exigences définies par les autorités compétentes et les cadres contractuels industriels, qui imposent des démarches formalisées de démonstration de conformité.

Voies d'accès

MODALITÉS D'ACCÈS

Formation initiale, Formation continue, Candidature individuelle, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

L'accès à la formation préparant au projet de certification est conditionné à la détention d'un titre ou diplôme de niveau 5 ou supérieur dans le domaine informatique, de la cybersécurité, de l'ingénierie ou d'un domaine connexe.

PRÉREQUIS À LA VALIDATION

Etre titulaire d'un diplôme ou titre de niveau 5 minimum dans les domaines de l'informatique, de la cybersécurité, de l'ingénierie ou d'un domaine connexe, et avoir une expérience professionnelle minimale de 2 ans dans le domaine de la cybersécurité justifiée par tous types de contrat y compris d'apprentissage.

Dans le cadre spécifique de la reconnaissance de l'expérience, être titulaire d'un diplôme ou titre de niveau 5 minimum dans les domaines de l'informatique, de la cybersécurité, de l'ingénierie ou d'un domaine connexe et justifier d'une expérience professionnelle minimale de 2 ans dans le domaine de la cybersécurité aéronautique et/ou spatiale.

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, CANDIDATURE INDIVIDUELLE

Le jury de certification est composé de 5 membres

: 2 représentants du certificateur, 3 professionnels externes exerçant dans le métier visé ou l'un des métiers visés par la certification ou supervisant des personnes qui l'exercent. Les membres du jury ne devront pas avoir de lien personnel ou professionnel avec un candidat. Les formateurs ne peuvent pas être membres du jury de certification.

COMPOSITION DU JURY — VAE

Le jury pour la reconnaissance de l'expérience est composé de 5 membres

: 2 représentants du certificateur, 3 professionnels externes exerçant dans le métier visé ou l'un des métiers visés par la certification ou supervisant des personnes qui l'exercent. Les membres du jury ne devront pas avoir de lien personnel ou professionnel avec un candidat. Les formateurs ne peuvent pas être membres du jury de certification.

Base légale

Date de décision	30/09/2026
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	30/09/2029
Date de dernière délivrance possible	30/03/2030

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2025	17	—	—	—

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/7741/>