

Technicien veilleur de cybersécurité

RNCP36164 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 5
Sigle	Autre — Autre certification professionnelle de droit
Code(s) NSF	326p
Formacode(s)	31045
Code(s) ROME	I1401, M1810, M1801
Type d'enregistrement	Enregistrement de droit
Date d'échéance	27/01/2027

Certificateur(s)

MINISTERE DES ARMEES · SIRET : 11009001600053

MINISTERE DES ARMEES · SIRET : 11009001600046

Partenaires habilités

6 organismes habilités, d'après la liste publiée par France compétences : 6 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
ÉCOLE DES TRANSMISSIONS (COMSIC-ETRS)	—	Former et organiser l'évaluation
LYCEE DES METIERS PIERRE MENDES FRANCE	19350030300030	Former et organiser l'évaluation
LYCEE DES METIERS YVES THEPOT	19290071000026	Former et organiser l'évaluation
LYCEE POLYVALENT CHAPTAL	19220058200026	Former et organiser l'évaluation
LYCEE POLYVALENT JEAN BAPTISTE COLBERT	19560026700049	Former et organiser l'évaluation
UNIVERSITE DE RENNES	13003051300019	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le personnel entrant au MINARM ne dispose généralement pas de qualifications ou compétences en matière de technique en veille de cybersécurité, ou insuffisamment. Le MINARM les lui fait donc acquérir afin de répondre à son propre besoin de techniciens veilleurs en cybersécurité. L'enregistrement dans le RNCP est une reconnaissance de la qualité des certifications délivrées au personnel, et par conséquent un gage d'attractivité comme de reclassement. Dans la société civile, la certification professionnelle de "technicien veilleur de cybersécurité" constitue une aide réelle à la reconversion car le secteur est très porteur d'emplois selon les données de l'observatoire des métiers du numérique (OPIIEC) : la cybersécurité est devenue un enjeu majeur pour toutes les organisations, qu'il s'agisse des entreprises ou des institutions publiques. Sur le segment de la cybersécurité industrielle, le marché de l'emploi est souvent décrit comme tendu et pénurique. L'accroissement des besoins en recrutement n'est pas le seul facteur explicatif de cette tension. Le manque de candidatures répondant aux besoins réels des entreprises et le peu de formation en cybersécurité industrielle sont également mis en avant pour expliquer le côté pénurique du marché. Cette pénurie est telle qu'elle pousse les entreprises à renoncer à recruter et à préférer une solution en interne. Si aujourd'hui la filière emploie déjà 24 000 salariés, dans les entreprises du numérique, de l'ingénierie, des études, du

conseil et de l'évènement, ce chiffre devrait bondir dans les prochaines années. À l'horizon de 3 ans, ces entreprises anticipent une croissance des effectifs en cybersécurité de 6 %, soit 1 400 créations nettes d'emplois. Une croissance qui atteint les 8 % de création nette d'emplois d'ici 5 ans.

ACTIVITÉS VISÉES

Le technicien veilleur de cybersécurité est responsable d'activités de support, de gestion ou d'administration de la sécurité d'un point de vue technique ou administratif : conception, production, conditionnement et gestion des réseaux de chiffrement et des éléments secrets.

Selon le profil d'emploi,

- il est en mesure de déployer et d'administrer des solutions de gestion de la sécurité, ainsi que de paramétrer les éléments de sécurité des équipements serveurs et des terminaux traitants ;
- il est en capacité d'effectuer des tâches de contrôle administratif de conformité dans les domaines des habilitations du personnel, du suivi comptable et des inventaires réglementaires, de l'application des procédures d'exploitation de sécurité, apportant ainsi son soutien aux opérations d'audit et de contrôle ;
- il participe à l'analyse de la vulnérabilité du système et des risques liés à la sécurité des données pour mettre en place un processus de protection ;
- il contribue aux séances de sensibilisation pour l'usage des ressources par les utilisateurs finaux ; - il participe à l'analyse d'une station de travail informatique compromise ou du moins suspectée de l'être.

Tel que pour la mise en œuvre dans le secteur civil, les principales activités du « technicien veilleur de cybersécurité » peuvent être présentées au sein de quatre blocs de compétences.

Bloc de compétences 1 : opérer le déploiement et l'administration d'une infrastructure sécurisée d'un système d'information en fonction des évolutions de l'organisme

Les activités principales composant ce bloc sont :

A1 – Déploiement de tout ou partie des architectures de sécurité des systèmes d'information, des réseaux de capteurs/actionneurs intelligents sécurisés, systèmes embarqués ou tout objet communicant sécurisé.

A2 – Conduite de l'administration et de l'évolution des équipements de sécurité.

Bloc de compétences 2 : superviser les réseaux et les systèmes d'information de l'infrastructure de l'organisme et assurer une veille technologique et réglementaire en matière de sécurité

Les activités principales composant ce bloc sont :

A1 – Supervision des réseaux.

A2 – Mise en place des veilles normatives, juridiques, gouvernementales et technologiques.

Bloc de compétences 3 : gérer les incidents de cybersécurité en assurant les premières réactions et investiguer ces événements de cybersécurité

Les activités principales composant ce bloc sont :

A1 – Gestion des événements de cybersécurité.

A2 – Investigation des événements de cybersécurité.

Bloc de compétences 4 : contrôler le droit d'accès au système et aux données de l'organisme, sensibiliser et former le personnel et conseiller l'officier de la sécurité des systèmes d'information de l'entreprise

Les activités principales composant ce bloc sont :

A1 – Participation au contrôle administratif et aux actions de conseil technique.

A2 – Collaboration au travail de sensibilisation et de formation de l'ensemble du personnel à l'hygiène informatique et aux risques liés à la cybersécurité et amélioration de ses compétences.

COMPÉTENCES ATTESTÉES

Bloc de compétences 1 : opérer le déploiement et l'administration d'une infrastructure sécurisée d'un système d'information en fonction des évolutions de l'organisme

Les compétences attestées composant ce bloc sont :

- Intégrer des équipements de sécurité (parefeu, sonde, IDS...) afin de créer une plateforme sécurisée répondant aux exigences de la politique de sécurité en vigueur au sein de l'organisme, en sélectionnant du matériel agréé ;
- Durcir les systèmes d'exploitation (Windows ou Linux) et la protection des postes de travail dans les domaines bureautique, scientifique et industriel en vue de maintenir l'intégrité des fonctionnalités et la fiabilité de l'ensemble du système, par l'application des paramétrages de sécurité recommandés, l'arrêt ou la désinstallation de services/logiciels et l'installation de logiciels de sécurité ;
- Gérer la sécurisation des flux dans l'intention d'assurer et d'améliorer la confidentialité, l'intégrité, la disponibilité des SI grâce à la réalisation d'une matrice des flux et la mise en place de la segmentation des réseaux ;
- Déployer les moyens cryptographiques adéquats pour assurer l'intégrité et la traçabilité des données

transmises/reçues dans le cadre de la défense en profondeur ;

- Anticiper les problèmes de fonctionnement des équipements de sécurité par la mise en place de parades technologiques aux incidents envisageables afin d'éviter le traitement des événements via l'application de procédures spécifiques aux dysfonctionnements ;
- Assurer le maintien en condition de sécurité (MCS) de l'ensemble des applications en mettant en oeuvre différents scénarios de gestion des correctifs de sécurité ou " patches" afin de certifier le bon niveau de sécurité de l'infrastructure de l'entreprise ;
- Réaliser des sauvegardes complètes et périodiques de l'infrastructure de l'organisme en vue de garantir une restauration rapide du SI suite à une attaque informatique ;
- Mettre en place les évolutions nécessaires pour garantir la sécurité logique et physique du SI par l'utilisation de matériels robustes et de moyens adaptés ;
- Contrôler méthodiquement le paramétrage de tous les dispositifs de sécurité déployés afin de garantir des applications et une infrastructure informatiques stables et sécurisées.

Bloc de compétences 2 : superviser les réseaux et les systèmes d'information de l'infrastructure de l'organisme et assurer une veille technologique et réglementaire en matière de sécurité

Les compétences attestées composant ce bloc sont :

- Analyser

les différentes remontées d'alertes issues des outils de détection et des comptes rendus afin de détecter les intrusions ou tentatives dans le système

grâce

à des outils d'analyse de données ou des corrélateurs d'événements ;

- Rechercher (via des outils d'analyse de log) les événements de cybersécurité et les menaces suite à un avis de sécurité afin de dépister une éventuelle intrusion ;
- Améliorer la supervision de sécurité par l'automatisation des outils de pilotage de la sécurité dans le but de rester réduire les tâches répétitives, chronophages et non essentielles ;
- Assurer la tenue des tableaux de bords relatifs à la sécurité du système d'information dans le but d'évaluer le niveau de performance et de sécurité et ainsi aider à la décision ;
- Appliquer les dispositions réglementaires et professionnelles en vigueur en matière de cybersécurité et de continuité d'activité au sein de son entité ;
- Assurer une veille sur les règlements et les standards liés aux évolutions législatives et réglementaires en se maintenant à jour des futures modifications afin d'anticiper les changements ;
- Assurer une veille réglementaire sur la protection des données personnelles (RGPD) dans une démarche de mise en conformité permanente vis-à-vis du RGPD et de maîtrise des enjeux majeurs (juridiques et financiers) liés à la protection des données personnelles ;
- Assurer une veille technologique en participant à des conférences ou des démonstrations techniques, en lisant des articles de presse écrite spécialisée ou en consultant des sites internet en matière de cybersécurité pour collecter les informations

utiles sur les nouveaux risques et nouvelles failles de sécurité.

Bloc de compétences 3 : gérer les incidents de cybersécurité en assurant les premières réactions et investiguer ces événements de cybersécurité

Les compétences attestées composant ce bloc sont :

- Caractériser un événement informatique en un incident de cybersécurité ou en une panne, un dysfonctionnement du système ;
- Opérer au sein de cellules opérationnelles de gestion de crise pour traiter l'incident le plus rapidement possible en mettant en oeuvre les actions décidées en réponse à l'incident afin que l'organisme reprenne son activité au plus tôt ;
- Mettre en oeuvre des solutions palliatives ou correctrices qui vont atténuer les conséquences de l'incident de cybersécurité et permettre une poursuite durable de l'activité ;
- Assurer le suivi des incidents en lien avec la cybersécurité en mettant à jour les différents tableaux de bord relatifs à l'activité de gestion des incidents ;
- Prélever les traces d'une attaque informatique passée ou en cours dans le but de fournir des preuves en cas d'une enquête interne à l'entreprise, voire judiciaire, à l'aide d'outils de forensique informatiques tout en préservant les données originales ;
- Analyser les prélèvements effectués afin de rechercher des indices d'une compromission du système ;
- Procéder à la création d'un laboratoire d'analyse pour une analyse de premier niveau permettant d'apporter les premiers éléments de preuve.

Bloc de compétences 4 : contrôler le droit d'accès au système et aux données de l'organisme, sensibiliser et former le personnel et conseiller l'officier de la sécurité des systèmes d'information de l'entreprise.

Les compétences attestées composant ce bloc sont :

- Attribuer les habilitations nécessaires aux collaborateurs et mener des revues d'habilitations régulières ou ponctuelles afin de s'assurer que tout le personnel de l'organisme a uniquement accès aux données dont il a besoin ;
- Conseiller les acteurs de la sécurité du patrimoine informationnel, sur les problématiques de sécurité dans leur domaine (production, développement, assistance) afin de contribuer à faire évoluer la sécurité selon les besoins et les risques ;
- Effectuer le suivi comptable des matériels afin d'avoir une vision en temps réel de l'état de son matériel et procéder aux inventaires réglementaires pour répertorier physiquement les équipements à l'aide d'outils spécifiques ;
- Sensibiliser, par le biais de campagnes de sensibilisation et de séances périodiques, les utilisateurs du système d'information à l'hygiène informatique, aux bonnes pratiques en termes de cybersécurité et aux risques induits afin qu'ils deviennent le maillon fort dans la lutte contre les menaces propres à leur environnement de travail ;
- Contribuer à la mise en œuvre de bonnes pratiques, en proposant de nouvelles procédures, de nouvelles actions qui pourront recueillir l'engagement de tous à respecter les règles de sécurité du système d'information notamment en lien avec la politique de cybersécurité de l'entreprise ;
- Mesurer

l'évolution du niveau de sensibilisation du personnel par le biais de mises en situation ou de questionnaires afin de consolider les résultats des différentes campagnes de cybersécurité.

Blocs de compétences

RNCP36164BC01 — Opérer le déploiement et l'administration d'une infrastructure sécurisée d'un système d'information en fonction des évolutions de l'organisme

LISTE DE COMPÉTENCES

- Intégrer des équipements de sécurité (parefeu, sonde, IDS...) afin de créer une plateforme sécurisée répondant aux exigences de la politique de sécurité en vigueur au sein de l'organisme, en sélectionnant du matériel agréé ;
- Durcir les systèmes d'exploitation (Windows ou Linux) et la protection des postes de travail dans les domaines bureautique, scientifique et industriel en vue de maintenir l'intégrité des fonctionnalités et la fiabilité de l'ensemble du système, par l'application des paramétrages de sécurité recommandés, l'arrêt ou la désinstallation de services/logiciels et l'installation de logiciels de sécurité ;
- Gérer la sécurisation des flux dans l'intention d'assurer et d'améliorer la confidentialité, l'intégrité, la disponibilité des SI grâce à la réalisation d'une matrice des flux et la mise en place de la segmentation des réseaux ;
- Déployer les moyens cryptographiques adéquats pour assurer l'intégrité et la traçabilité des données transmises/reçues dans le cadre de la défense en profondeur ;
- Anticiper les problèmes de fonctionnement des équipements de sécurité par la mise en place de parades technologiques aux incidents envisageables afin d'éviter le traitement des événements via l'application de procédures spécifiques aux dysfonctionnements ;
- Assurer le maintien en condition de sécurité (MCS) de l'ensemble des applications en mettant en œuvre différents scénarios de gestion des correctifs de sécurité ou « patches » afin de certifier le bon niveau de sécurité de l'infrastructure de l'entreprise ;
- Réaliser des sauvegardes complètes et périodiques de l'infrastructure de l'organisme en vue de garantir une restauration rapide du SI suite à une attaque informatique ;
- Mettre en place les évolutions nécessaires pour garantir la sécurité logique et physique du SI par l'utilisation de matériels robustes et de moyens adaptés ;
- Contrôler méthodiquement le paramétrage de tous les dispositifs de sécurité déployés afin de garantir des applications et une infrastructure informatiques stables et sécurisées.

MODALITÉS D'ÉVALUATION

Voie formative:

- contrôles de connaissances ;
- mise en situation contextualisée;
- étude cas et/ou de restitutions technico-opérationnelles

VAE

- étude du livret 2 ;
- entretien avec le jury ;
- mise en situation simulée ou réelle, si nécessaire

RNCP36164BC02 — Superviser les réseaux et systèmes d'information de l'infrastructure de l'organisme et assurer une veille technologique et réglementaire en matière de sécurité

LISTE DE COMPÉTENCES

- Analyser

les différentes remontées d'alertes issues des outils de détection et des comptes rendus afin de détecter les intrusions ou tentatives dans le système

grâce

à des outils d'analyse de données ou des corrélateurs d'événements ;

- Rechercher (via des outils d'analyse de log) les événements de cybersécurité et les menaces suite à un avis de sécurité afin de dépister une éventuelle intrusion ;
- Améliorer la supervision de sécurité par l'automatisation des outils de pilotage de la sécurité dans le but de rester réduire les tâches répétitives, chronophages et non essentielles ;
- Assurer la tenue des tableaux de bords relatifs à la sécurité du système d'information dans le but d'évaluer le niveau de performance et de sécurité et ainsi aider à la décision ;
- Appliquer les dispositions réglementaires et professionnelles en vigueur en matière de cybersécurité et de continuité d'activité au sein de son entité ;
- Assurer une veille sur les règlements et les standards liés aux évolutions législatives et réglementaires en se maintenant à jour des futures modifications afin d'anticiper les changements ;
- Assurer une veille réglementaire sur la protection des données personnelles (RGPD) dans une démarche de mise en conformité permanente vis-à-vis du RGPD et de maîtrise des enjeux majeurs (juridiques et financiers) liés à la protection des données personnelles ;
- Assurer une veille technologique en participant à des conférences ou des démonstration techniques, en lisant des articles de presse écrite spécialisée ou en consultant des sites internet en matière de cybersécurité pour collecter les informations utiles sur les nouveaux risques et nouvelles failles de sécurité.

MODALITÉS D'ÉVALUATION

Voie formative:

- contrôles de connaissances ;
- mise en situation contextualisée;
- étude cas et/ou de restitutions technico-opérationnelles

VAE

- étude du livret 2 ;
- entretien avec le jury ;
- mise en situation simulée ou réelle, si nécessaire

RNCP36164BC03 — Gérer les incidents de cybersécurité en assurant les premières réactions et investiguer ces événements de cybersécurité

LISTE DE COMPÉTENCES

- Caractériser un événement informatique en un incident de cybersécurité ou en une panne, un dysfonctionnement du système ;
- Opérer au sein de cellules opérationnelles de gestion de crise pour traiter l'incident le plus rapidement possible en mettant en œuvre les actions décidées en réponse à incident afin que l'organisme reprenne son activité au plus tôt ;
- Mettre en œuvre des solutions palliatives ou correctrices qui vont atténuer les conséquences de l'incident de cybersécurité et permettre une poursuite durable de l'activité ;
- Assurer le suivi des incidents en lien avec la cybersécurité en mettant à jour les différents tableaux de bord relatifs à l'activité de gestion des incidents ;
- Prélever les traces d'une attaque informatique passée ou en cours dans le but de fournir des preuves en cas d'une enquête interne à l'entreprise, voire judiciaire, à l'aide d'outils de forensique informatiques tout en préservant les données originales ;

- Analyser les prélèvements effectués afin de rechercher des indices d'une compromission du système ;
- Procéder à la création d'un laboratoire d'analyse pour une analyse de premier niveau permettant d'apporter les premiers éléments de preuve.

MODALITÉS D'ÉVALUATION

Voie formative:

- contrôles de connaissances ;
- mise en situation contextualisée;
- étude cas et/ou de restitutions technico-opérationnelles

VAE

- étude du livret 2 ;
- entretien avec le jury ;
- mise en situation simulée ou réelle, si nécessaire

RNCP36164BC04 — Contrôler le droit d'accès au système et aux données, sensibiliser et former les personnels et conseiller l'officier de sécurité des systèmes d'information de l'entreprise

LISTE DE COMPÉTENCES

- Attribuer les habilitations nécessaires aux collaborateurs et mener des revues d'habilitations régulières ou ponctuelles afin de s'assurer que tout le personnel de l'organisme a uniquement accès aux données dont il a besoin ;
- Conseiller les acteurs de la sécurité du patrimoine informationnel, sur les problématiques de sécurité dans leur domaine (production, développement, assistance) afin de contribuer à faire évoluer la sécurité selon les besoins et les risques ;
- Effectuer le suivi comptable des matériels afin d'avoir une vision en temps réel de l'état de son matériel et procéder aux inventaires réglementaires pour répertorier physiquement les équipements à l'aide d'outils spécifiques ;
- Sensibiliser, par le biais de campagnes de sensibilisation et de séances périodiques, les utilisateurs du système d'information à l'hygiène informatique, aux bonnes pratiques en termes de cybersécurité et aux risques induits afin qu'ils deviennent le maillon fort dans la lutte contre les menaces propres à leur environnement de travail ;
- Contribuer à la mise en œuvre de bonnes pratiques, en proposant de nouvelles procédures, de nouvelles actions qui pourront recueillir l'engagement de tous à respecter les règles de sécurité du système d'information notamment en lien avec la politique de cybersécurité de l'entreprise ;
- Mesurer

l'évolution du niveau de sensibilisation du personnel par le biais de mises en situation ou de questionnaires afin de consolider les résultats des différentes campagnes de cybersécurité.

MODALITÉS D'ÉVALUATION

Voie formative:

- contrôles de connaissances ;
- mise en situation contextualisée;
- étude cas et/ou de restitutions technico-opérationnelles

VAE

- étude du livret 2 ;
- entretien avec le jury ;
- mise en situation simulée ou réelle, si nécessaire

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Au sein du ministère des armées, le technicien veilleur de cybersécurité est principalement en fonction au sein des DIRISI régionales (BORDEAUX, LYON, METZ, LILLE, TOULON, BREST et RENNES), dans les régiments de transmissions, ainsi que dans les entités cyberdéfense (807 CT, CASSI, CALID).

Le détenteur de la certification exerce les fonctions de sécurisation des systèmes d'information ou des bases de données déployés, à la fois au profit du commandement en opération et au profit de tous les utilisateurs en garnison. Par la suite, il peut prétendre aux postes d'administrateur dans ce domaine. Ses activités se situent autour des

équipements et des réglementations que constitue tout système sécurisé. Dans certaines situations, l'activité peut s'exercer en horaires décalés, par roulement et être soumis un régime d'astreinte.

Dans le secteur civil, les techniciens veilleurs de cybersécurité peuvent être employés dans des organisations de différentes tailles qu'il s'agisse des entreprises privées ou institutions publiques dont le secteur d'activité relève du domaine du déploiement de solutions de sécurisation ou de la mise en œuvre d'un centre de supervision de la sécurité (SOC). Les « techniciens veilleur de cybersécurité » peuvent être embauchés dans des sociétés d'audit, de consulting, d'édition de logiciels de sécurité ou encore au sein des services sécurité des systèmes d'information internes des entreprises des secteurs d'activité sensible tels que la banque/finance, la défense ou encore les systèmes industriels de production.

TYPE D'EMPLOIS ACCESSIBLES

Cette appellation renvoie au ministère des armées aux libellés d'emploi suivants:

- Technicien cybersécurité ;
- Technicien sécurité ;
- Technicien veilleur Cyberdéfense.

Cette appellation renvoie dans le secteur civil aux intitulés suivants:Technicien support SSI ;

- Technicien support Specialist ;
- Administrateur (trice) sécurité ;
- Technicien informatique, spécialisé en cybersécurité des PME.

RÈGLEMENTATIONS D'ACTIVITÉ

- Le personnel accédant à la certification professionnelle par la voie de la formation doit détenir une habilitation "confidentiel défense" (CD). Dès le début du stage, le stagiaire devra présenter son certificat de sécurité CD.
- L'obtention de la certification professionnelle inscrite dans le RNCP ne permet pas à elle seule d'exercer au sein du ministère des armées le métier qu'elle vise ; le statut de personnel militaire ou civil des Armées est exigé.

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Modérée (3/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 4 sur 5.
Facteurs principaux	Intensité d'embauche, Inadéquation géographique
Salaire médian (mensuel)	2 419 €
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom · tension 3/5 (Modérée)
Projets de recrutement (BMO 2026)	9 549
Jugés difficiles à recruter	46 %
Emplois saisonniers	3 %
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Pour prétendre à la certification professionnelle enregistrée dans le RNCP, le stagiaire doit d'abord satisfaire tous les conditions d'accès aux formations de spécialité en cybersécurité permettant d'acquérir les compétences de la

certification, puis suivre avec succès ces formations et détenir les compétences telles que définies dans les référentiels de certification.

COMPOSITION DU JURY — FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION

Jury de certification hors VAE

Le jury de certification (hors VAE) pourra comprendre jusqu'à cinq membres avec, si possible, une représentation équilibrée des hommes et des femmes :

- un président assisté de :
- deux membres du « collège professionnels » ;
- deux membres du « collège formateurs ».

Des suppléants sont également désignés.

Le président du jury de certification (hors VAE) est soit le commandant de l'école des transmissions, soit le directeur de l'enseignement ou un officier supérieur cadre de l'enseignement. Le président et les membres du jury (ainsi que les suppléants) sont désignés par le commandant de l'organisme certificateur pour une période d'un an renouvelable.

Le jury de certification (hors VAE) pourra être réduit à trois membres avec, si possible, une représentation équilibrée des hommes et des femmes. Dans ce cas, il devra comprendre au moins 2 professionnels du secteur :

- Président du jury (hors VAE) : le commandant de l'école des transmissions en qualité de professionnel du secteur ou son représentant (non formateur) ;
- 1 deuxième représentant qualifié de la profession (non formateur) ;
- 1 troisième représentant qualifié de la profession (non formateur) ou un formateur.

Les « professionnels » sont représentés par tout professionnel du secteur hors formateurs, hors organisme certificateur si possible.

Pourcentage de membres extérieurs à l'autorité délivrant la certification dont professionnels qualifiés :

50 %

dans la mesure

du possible, hormis le président

COMPOSITION DU JURY — VAE

Jury de certification VAE

Nombre et profils des personnes composant le jury : 3, jusqu'à 5

Le jury de certification par voie de VAE pourra comprendre jusqu'à cinq membres avec, si possible, une représentation équilibrée des hommes et des femmes :

- Président du jury de VAE : le commandant de l'école des transmissions ou son représentant en qualité de professionnel du secteur ;
- deux membres du « collège professionnels » ;
- deux membres du « collège formateurs ».

Des suppléants sont désignés.

Le président et les membres du jury de VAE (ainsi que les suppléants) sont désignés par le chef d'établissement de l'organisme certificateur pour une période d'un an renouvelable.

Selon les situations, le jury de VAE pourra être composé de trois membres avec, si possible, une représentation équilibrée des hommes et des femmes. Dans ce cas, il devra comprendre au moins 2 professionnels du secteur :

- Président du jury : le commandant de l'école des transmissions en qualité de professionnel du secteur ou son représentant (non formateur) ;
- 1 deuxième représentant qualifié de la profession (non formateur) ;
- 1 troisième représentant qualifié de la profession (non formateur) ou un formateur. Les « professionnels » sont représentés par tout professionnel hors formateurs, hors organisme certificateur si possible.

Les « professionnels » sont représentés par tout professionnel hors formateurs, hors organisme certificateur si possible.

Pourcentage de membres extérieurs à l'autorité délivrant la certification dont professionnels qualifiés :

50 %

dans la mesure du possible, hormis le président

Financement en alternance (NPEC)

Niveau de prise en charge d'un contrat d'apprentissage par les OPCO, fixé par France compétences par branche professionnelle (CPNE).

Prise en charge usuelle 9 424 €

Selon la branche 6 600 € – 9 424 €

Prise en charge	Branches concernées
9 424 €	Valeur par défaut · 203 branches
9 055 €	CPNEFP Grands Magasins/ Magasins Populaires, CPNEFP Habillement succursaliste, CPNEFP du Négoce de l'ameublement
9 155 €	CPNE de la branche de l'hospitalisation privée à statut commercial et du thermalisme
9 047 €	CPNEFP de l'enseignement privé indépendant
9 046 €	CPNE Travail Temporaire
8 575 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
8 303 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
8 300 €	CPNEFP Commerce à distance
6 600 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager

Base légale

Date d'échéance de l'enregistrement 27/01/2027

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2020	10	0	100 %	—

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/36164/>