

Expert réseaux infrastructures et sécurité

RNCP39781 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326, 326n
Formacode(s)	24273, 31094, 31006, 31034
Code(s) ROME	M1801, M1802, M1803, M1806, M1810
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	31/10/2024
Date d'échéance	31/10/2029

Certificateur(s)

ASSOCIATION POUR LA GESTION DE 3IL · SIRET : 39770462800015

Partenaires habilités

27 organismes habilités, d'après la liste publiée par France compétences : 27 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
ASSOCIATION O.R.T.	77568810400063	Former et organiser l'évaluation
ASSOCIATION SAINTE ANGELE	78071371500107	Former et organiser l'évaluation
CAMPUS DE MONTPELLIER	92369614000022	Former et organiser l'évaluation
CFAI POITOU-CHARENTES	33811430900010	Former et organiser l'évaluation
CFT TUNIS	—	Former et organiser l'évaluation
CHAMBRE DE COMMERCE ET D INDUSTRIE	18974211700097	Former et organiser l'évaluation
CHAMBRE DE COMMERCE ET D INDUSTRIE DU TARN (CCI) - SITE DE CASTRES MAZAMET	13001278400026	Former et organiser l'évaluation
ECOLE 18.06 ALSACE	94480869000027	Former et organiser l'évaluation
ECOLE SUPERIEURE DU NUMERIQUE DES LANDES	90111295300012	Former et organiser l'évaluation
EFREI PARIS	39889833800023	Former et organiser l'évaluation

Liste complète des 27 partenaires habilités : <https://data.aktaconseil.fr/certifications/rncp39781-expert-reseaux-infrastructures-et-securite/partenaires>

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'Expert Réseaux Infrastructures et Sécurité fait partie de la sphère des administrateurs systèmes en tant que responsable d'infrastructure. A ce titre, son premier rôle consiste à répondre à chaque besoin métier de l'entreprise, exprimé par la direction/DSI, au moyen d'une solution technique qu'il aura conçue, mettant principalement en jeu des équipements réseaux et des serveurs physiques ou virtuels, sur lesquels il va déployer et configurer des systèmes d'exploitation, applicatifs et services, tout en veillant à la sécurité de l'ensemble. Il a donc en charge la conception de la solution, et, selon la taille de l'entreprise, sa contribution à la mise en œuvre peut aller de la réalisation complète au pilotage d'une équipe.

ACTIVITÉS VISÉES

Participation à la définition des politiques de gouvernance de l'infrastructure
Contrôle de la conformité réglementaire
Gestion des contrats de services ou SLA (Service Level Agreements)
Mise en œuvre des Plans de Continuité (PCA) et de Reprise d'Activité (PRA)
Promotion et intégration du Numérique Responsable
Conception d'architectures systèmes et réseaux
Gestion et Supervision de la Mise en Œuvre de l'Infrastructure (MOE)
Gestion des incidents et des tickets
Elaboration d'une politique de sécurité des SI
Formation et Sensibilisation à la Cybersécurité
Evaluation de la sécurité : Ethical Hacking et tests de pénétration
Investigation et Analyse des Incidents de Sécurité : Analyse Forensic
Supervision et Gestion des Centres Opérationnels de Sécurité (SOC)
Pilotage de projets
Gestion du Changement et de la Transformation IT
Accompagnement et Développement des équipes projets

COMPÉTENCES ATTESTÉES

Participer aux politiques de gouvernance IT dans le cadre du schéma directeur de la DSI pour garantir que la gestion l'infrastructure répondent aux exigences de performance, de sécurité et de conformité
Auditer l'infrastructure de l'entreprise pour contrôler la conformité réglementaire
Etablir des accords de niveaux de service (SLA) afin d'offrir des prestations ou des réalisations répondant aux exigences et objectifs de l'entreprise
Elaborer, documenter et mettre en œuvre des processus et procédures standardisées pour garantir la qualité et l'efficacité des services
Analyser les causes de non-respect des SLA afin de proposer des actions correctives
Evaluer les risques pesant sur la production en lien avec l'informatique afin de définir et documenter des plans de continuité et de reprise de l'activité
Elaborer un plan de continuité d'activité (PCA) afin de respecter le niveau de service contractuel
Définir un plan de reprise d'activité (PRA) afin d'assurer une protection optimale contre les risques de perte de données, et permettre une récupération rapide et efficace en cas de sinistre
Etablir et mettre en œuvre des tests des plans de continuité (PCA) et des plans de reprise d'activité (PRA) afin d'améliorer la préparation aux incidents et assurer la résilience des infrastructures systèmes et réseaux
Mettre en œuvre le Numérique Responsable afin de mesurer et d'améliorer la performance environnementale du SI et les pratiques RSE afférentes
Concevoir une infrastructure système et réseau optimisée et sécurisée afin de fournir une base technique robuste et efficace soutenant les opérations de l'entreprise tout en garantissant la sécurité des données et des communications
Définir, implémenter et contrôler les règles d'accès aux données et aux services afin de protéger les systèmes et les données sensibles contre les accès non autorisés
Arbitrer la technologie d'hébergement des systèmes et/ou applications (serveur dédié, virtualisation, conteneurisation/orchestration ou cloud) pour les déployer, les mettre en production et les gérer de manière fiable, flexible et scalable
Concevoir une topologie des réseaux de l'entreprise tant mono que multisites, afin de garantir la qualité de service (QoS), la résilience (PCA) et la sécurité des communications

Contribuer à la mise en place, au contrôle et à l'administration de l'infrastructure, pour déployer les éléments techniques de la solution

Automatiser les processus d'intégration, de déploiement et de maintenance des systèmes et applications pour assurer la fiabilité et la reproductibilité des mises en production

Organiser et piloter la gestion des incidents et du support pour suivre, prioriser et résoudre les incidents, ainsi qu'assurer une résolution rapide et efficace des problèmes techniques

Elaboration d'une politique de sécurité des SI

Conduire une veille active afin d'anticiper les menaces et vulnérabilités émergentes et mener des actions correctives

Participer à l'élaboration et à la mise en œuvre de la Politique de Sécurité des Systèmes d'Information (PSSI) de l'entreprise, pour protéger les données et les systèmes de l'entreprise

Auditer la sécurité en collaboration avec le Responsable de la Sécurité des Systèmes d'Information (RSSI) afin de vérifier la mise en œuvre de la politique de sécurité et assurer son amélioration continue

Sensibiliser le personnel aux bonnes pratiques de la sécurité informatique afin de diminuer les comportements à risques et de contribuer à l'amélioration continue de la sécurité de l'entreprise

Eprouver la sécurité de l'infrastructure afin d'évaluer la robustesse des systèmes et la réactivité des équipes

Investiguer et analyser les incidents de sécurité, afin de préparer des rapports en vue des audits de sécurité et conserver des preuves légales

Contribuer au fonctionnement du Centre Opérationnel de Sécurité (SOC), afin de maintenir la sécurité et la résilience de l'infrastructure

Piloter un projet pour gérer les équipes, s'assurer que les solutions déployées répondent aux attentes de l'entreprise et garantir la qualité des livrables, le respect des délais et des coûts

Assurer le suivi et le reporting du projet afin de garantir une communication claire, efficace et adaptée aux besoins, de faciliter la prise de décision, d'assurer la transparence sur l'avancement du projet, et de maintenir l'alignement des objectifs

Elaborer et mettre en œuvre la conduite du changement afin de minimiser l'impact d'une évolution (mineure, delta ou majeure) de l'infrastructure sur l'environnement de production

Développer la performance de l'équipe pour améliorer la réussite des projets dans le respect des exigences fixées

Contribuer au recrutement des collaborateurs afin de contribuer à la construction d'une équipe diversifiée, reflétant les valeurs de l'égalité des chances et de la responsabilité sociétale (RSE)

Blocs de compétences

RNCP39781BC01 — Gouverner les Infrastructures Systèmes et Réseaux

LISTE DE COMPÉTENCES

Participer aux politiques de gouvernance IT dans le cadre du schéma directeur de la DSI, en s'appuyant sur des référentiels de bonnes pratiques, en mobilisant son expertise technique, et en contribuant à la structuration de la gestion des services IT, pour garantir que la gestion l'infrastructure répondent aux exigences de performance, de sécurité et de conformité

Auditer l'infrastructure de l'entreprise en évaluant systématiquement les volets techniques et organisationnels à l'aide de méthodes d'analyse, d'outils de surveillance et de cadres de référence pour contrôler la conformité réglementaire

Etablir des accords de niveaux de service (SLA) en collaboration avec les clients internes et/ou externes, en définissant des indicateurs clés de performance (KPI) et leurs valeurs cibles associées, réunis en tableaux de bord et en utilisant des outils de gestion de SLA, afin d'offrir des prestations ou des réalisations répondant aux exigences et objectifs de l'entreprise

Elaborer, documenter et mettre en œuvre des processus et procédures standardisées en s'appuyant sur des normes et/ou référentiels tels que ISO 9001 et ITIL pour garantir la qualité et l'efficacité des services

Analyser les causes de non-respect des SLA en s'appuyant sur les KPI et des outils d'audit et d'analyse de données afin de proposer des actions correctives

Evaluer les risques pesant sur la production en lien avec l'informatique, en identifiant les menaces, en évaluant leurs probabilités et impacts afin de définir et documenter des plans de continuité et de reprise de l'activité

Elaborer un plan de continuité d'activité (PCA) en s'appuyant sur les SLA et l'analyse de risques, en produisant sa documentation et en définissant les moyens humains et techniques nécessaires à sa mise en place afin de respecter le niveau de service contractuel

Définir un plan de reprise d'activité (PRA) en priorisant les applications et services critiques et en établissant des

stratégies de sauvegarde, avec respect du principe du 3-2-1, et de restauration, aussi bien matérielle et/ou logicielle qu'organisationnelle, afin d'assurer une protection optimale contre les risques de perte de données, et permettre une récupération rapide et efficace en cas de sinistre

Etablir et mettre en œuvre des tests des plans de continuité (PCA) et des plans de reprise d'activité (PRA) en simulant des situations de crise réelle ou de pannes majeures sous forme d'exercices réflexifs, pratiques ou simulés afin d'améliorer la préparation aux incidents et assurer la résilience des infrastructures systèmes et réseaux

Mettre en œuvre le Numérique Responsable en adaptant des pratiques durables et d'accessibilité (personnes en situation de handicap), en se basant sur l'inventaire exhaustif des actifs informatiques et en utilisant les outils de référence afin de mesurer et d'améliorer la performance environnementale du SI et les pratiques RSE afférentes

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle simulée à partir d'un scénario d'entreprise fictive dont il faut gérer les services informatiques.

Préparation collective des livrables écrits et oral individuel

RNCP39781BC02 — Concevoir et Piloter les Infrastructures Systèmes et Réseaux

LISTE DE COMPÉTENCES

Concevoir une infrastructure système et réseau optimisée et sécurisée en analysant les besoins métiers et en proposant des solutions, en conformité avec le schéma directeur de la DSI, en combinant des ressources locales (on-premise) et/ou Cloud (SaaS, PaaS, IaaS) afin de fournir une base technique robuste et efficace soutenant les opérations de l'entreprise tout en garantissant la sécurité des données et des communications

Définir, implémenter et contrôler les règles d'accès aux données et aux services en retranscrivant les règles métiers dans une solution de gestion des identités (IAM*) afin de protéger les systèmes et les données sensibles contre les accès non autorisés

Arbitrer la technologie d'hébergement des systèmes et/ou applications (serveur dédié, virtualisation, conteneurisation/orchestration ou cloud) en évaluant et optimisant les ressources nécessaires à leur usage (telles que machine, stockage, bande passante, processeur, mémoire, consommation électrique), pour les déployer, les mettre en production et les gérer de manière fiable, flexible et scalable

Concevoir une topologie des réseaux de l'entreprise tant mono que multisites, en tenant compte des engagements de disponibilité, de capacité afin de garantir la qualité de service (QoS), la résilience (PCA) et la sécurité des communications

Contribuer à la mise en place, au contrôle et à l'administration de l'infrastructure, en mobilisant ses compétences techniques, en collaborant avec les équipes pluridisciplinaires et en documentant la solution pour déployer les éléments techniques de la solution

Automatiser les processus d'intégration, de déploiement et de maintenance des systèmes et applications en utilisant des outils d'orchestration, de gestion de déploiement et de DevOps et en contrôlant le résultat par l'analyse des logs produits pour assurer la fiabilité et la reproductibilité des mises en production

Organiser et piloter la gestion des incidents et du support en définissant les processus standardisés pour la création, l'attribution, le suivi des tickets et leur élévation, dans un cadre d'amélioration continue et en s'appuyant sur des outils de gestion des tickets (ITSM), pour suivre, prioriser et résoudre les incidents, ainsi qu'assurer une résolution rapide et efficace des problèmes techniques

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle simulée de montage d'infrastructure

Mise en situation professionnelle – étude de cas sur l'organisation de la gestion des incidents et du support

RNCP39781BC03 — Piloter la Sécurité des Systèmes d'Information

LISTE DE COMPÉTENCES

Conduire une veille active en matière de cybersécurité, en analysant régulièrement les bulletins de sécurité, les publications des organismes de référence tant francophones qu'anglophones et en partageant les fruits de ses recherches conformément aux us de l'équipe (rapport/article, réseau social interne, plateforme collaborative), afin d'anticiper les menaces et vulnérabilités émergentes et mener des actions correctives

Participer à l'élaboration et à la mise en œuvre de la Politique de Sécurité des Systèmes d'Information (PSSI) de l'entreprise, en s'appuyant sur les standards, en s'appuyant sur une analyse des risques de sécurité, en définissant des mesures, rôles, responsabilités, procédures et protocoles, en collaboration avec le Responsable de la Sécurité des Systèmes d'Information (RSSI) pour protéger les données et les systèmes de l'entreprise

Auditer la sécurité en collaboration avec le Responsable de la Sécurité des Systèmes d'Information (RSSI) en couvrant les volets organisationnels, physiques et techniques afin de vérifier la mise en œuvre de la politique de sécurité et assurer son amélioration continue

Sensibiliser le personnel aux bonnes pratiques de la sécurité informatique en conformité avec les préconisations de l'ANSSI au moyen d'ateliers, de documentation, d'exercices de simulation d'attaque, et de campagnes de phishing afin de diminuer les comportements à risques et de contribuer à l'amélioration continue de la sécurité de l'entreprise

Eprouver la sécurité de l'infrastructure sous la responsabilité du RSSI, au moyen de tests de pénétration, de simulations d'attaques, d'outils d'analyse de sécurité afin d'évaluer la robustesse des systèmes et la réactivité des équipes

Investiguer et analyser les incidents de sécurité, en conformité avec les recommandations de l'ANSSI, en examinant les systèmes compromis, en retraçant les actions malveillantes, et en collectant les preuves numériques afin de préparer des rapports en vue des audits de sécurité et conserver des preuves légales

Contribuer au fonctionnement du Centre Opérationnel de Sécurité (SOC), en gérant les incidents de sécurité au moyen de solutions SIEM, en analysant les données de sécurité, en détectant les anomalies, en orchestrant des réponses rapides et efficaces, en pilotant le déploiement des correctifs, s'il y a lieu de façon automatisée, et en assurant une surveillance continue afin de maintenir la sécurité et la résilience de l'infrastructure

MODALITÉS D'ÉVALUATION

Rapport de veille sur la cybersécurité en anglais

Mise en situation professionnelle simulée – rédaction d'une politique de sécurité

Mise en situation professionnelle – Etude de cas écrite sur la base d'un rapport d'audit

RNCP39781BC04 — Piloter les Projets et la Conduite du Changement

LISTE DE COMPÉTENCES

Piloter un projet au moyen d'une méthode de gestion de projet et des outils adaptés au contexte, en analysant le besoin, en rédigeant les documents d'initialisation et de suivi de projet adaptés à la méthode, en mobilisant les ressources et moyens nécessaires, pour gérer les équipes, s'assurer que les solutions déployées répondent aux attentes de l'entreprise et garantir la qualité des livrables, le respect des délais et des coûts

Assurer le suivi et le reporting du projet en s'adaptant aux parties prenantes concernées (COFIL, équipe projet, client) afin de garantir une communication claire, efficace et adaptée aux besoins, de faciliter la prise de décision, d'assurer la transparence sur l'avancement du projet, et de maintenir l'alignement des objectifs

Elaborer et mettre en œuvre la conduite du changement en s'appuyant sur des référentiels tels qu'ITIL, en réalisant une analyse de risques, en mettant au point une procédure de mise en production et au moyen de documentations et/ou de formations pour les utilisateurs concernés (acteurs comme usagers), afin de minimiser l'impact d'une évolution (mineure, delta ou majeure) de l'infrastructure sur l'environnement de production

Développer la performance de l'équipe en identifiant les besoins en compétences, en développant les talents, en planifiant la formation des collaborateurs, en participant à leur évaluation, et en mesurant l'écart entre les objectifs et le réalisé, pour améliorer la réussite des projets dans le respect des exigences fixées

Contribuer au recrutement des collaborateurs en participant aux rédactions de fiches de poste, en assurant une caution technique au moyen d'évaluations des compétences lors des entretiens, et en mettant l'accent sur l'inclusion notamment des personnes en situation de handicap, afin de contribuer à la construction d'une équipe diversifiée, reflétant les valeurs de l'égalité des chances et de la responsabilité sociétale (RSE)

MODALITÉS D'ÉVALUATION

Mise en situation reconstituée

Etude de cas portant sur un scénario de la mutation d'une entreprise sur la base d'un gros changement IT

Epreuve écrite suivie d'un oral

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

L'Expert Réseaux Infrastructure et Sécurité a pour fonction principale la conception, la gestion et la sécurisation d'un système d'information. De ce fait, il peut exercer au sein de toute organisation utilisant un système d'information, quel que soit le secteur, la taille ou la nature de cette organisation. Il peut aussi trouver naturellement place au sein des ESN qui ont pour mission d'effectuer des prestations concernant les systèmes d'information de leurs entreprises clientes.

TYPE D'EMPLOIS ACCESSIBLES

Responsable informatique
Consultant informatique
Ingénieur sécurité informatique
Consultant IT
Responsable des systèmes d'information
Expert en cybersécurité
Chef de projet informatique
Responsable sécurité informatique
Responsable sécurité des systèmes d'information
Expert système et réseaux
Administrateur système informatique
Expert sécurité informatique
Administrateur sécurité informatique
Ingénieur système informatique

RÈGLEMENTATIONS D'ACTIVITÉ

Bien que la profession d'expert réseaux infrastructures et sécurité ne soit pas réglementée spécifiquement, les activités liées au domaine du numérique sont strictement encadrées par la législation en vigueur concernant le traitement des données personnelles et la sécurité numérique. Ces activités doivent se conformer aux lois relatives à la protection de la vie privée, y compris le Règlement Général sur la Protection des Données (RGPD) et les obligations de déclaration à la CNIL.

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)	Élevée (4/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 942 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (19 % des actifs en emploi)
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) M2X91 — Chefs de projet et directeurs de service 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) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	16 497
Jugés difficiles à recruter	46 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X91 — Chefs de projet et directeurs de service informatique M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Cursus en 3 ans, être titulaire d'une certification de niveau 5 dans le domaine informatique.

Cursus en 2 ans : être titulaire d'une certification de niveau 6 dans le domaine informatique.

Procédure dérogatoire : Pour les candidats ne disposant pas d'un niveau de qualification suffisant ou issue d'un autre secteur, ces derniers peuvent accéder au parcours certifiant après avoir passé les tests d'inscription, rédigé une lettre de motivation et avoir effectué un entretien de sélection avec le responsable des admissions afin de valider leur pré-requis.

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

Le jury de certification est composé de 4 membres dont 2 personnalités extérieures (a minima 50%) travaillant dans le domaine d'activité de la certification et justifiant d'au moins 5 ans d'expérience, sans lien ni avec les candidats ni avec l'organisme certificateur

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	8 638 €
Selon la branche	7 000 € – 8 668 €
Prise en charge	Branches concernées
8 638 €	Valeur par défaut · 196 branches
8 668 €	CPNE autoroutes, CPNE de l'ingénierie, des services informatiques et du conseil, CPNE de la branche de l'hospitalisation privée à statut commercial et du thermalisme, CPNEFP dans les établissements d'enseignement privés sous contrat, CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager
8 460 €	CPNE industries alimentaires diverses, CPNEFP ICGV entreprises de la viande, CPNEFP de la branche des industries de produits alimentaires élaborés, CPNEFP dans la coopération agricole
8 000 €	CPNE des industries de santé (CPNEIS), CPNEF inter-secteurs papier carton
8 651 €	CPNE des Télécoms
8 600 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
8 500 €	CPNEFP de la métallurgie
8 250 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
7 000 €	CPNEFP de l'enseignement privé indépendant

Base légale

Date de décision	31/10/2024
Durée de l'enregistrement	5 ans
Date d'échéance de l'enregistrement	31/10/2029
Date de dernière délivrance possible	31/10/2033

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
--------------	------------------	-----------------	-------------------------	---------------------

2022	100	1	96 %	86 %
2021	41	3	97 %	74 %
2020	37	0	83 %	75 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP34407

CORRESPONDANCES (PAR BLOCS)

RNCP34407, RNCP36296, RNCP38105, RNCP38117, RNCP38779, RNCP38823

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.3il-ingenieurs.fr/nos-masteres/mastere-expert-reseaux-infrastructures-et-securite-eris/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/39781/>

Où se former

Formations référencées	10
Organismes	4
Régions couvertes	4
Prix indicatif	2 000 € – 18 000 €
Durée	75 – 963 h

Offre de formation — MonCompteFormation (Caisse des Dépôts), licence ouverte.

Se former en apprentissage

Formations en apprentissage	15
Organismes gestionnaires (CFA)	13
Organismes formateurs	13
Régions couvertes	8
Départements couverts	13
Organismes certifiés Qualiopi	13
Sessions	de 10/2024 à 09/2029

Catalogue des formations en apprentissage — réseau des Carif-Oref. Sans frais pour l'alternant : formation financée par l'OPCO de la branche (NPEC).

Entrées et sorties de formation

Entrées en formation	1
Parcours menés à terme	0
Taux d'achèvement	0 %

Entrées et sorties — Caisse des Dépôts (open data), tous organismes confondus.

Demande CPF — formations engagées

Dossiers CPF engagés	4
Montant total engagé	11 271 €
Coût moyen par dossier	2 818 €
Durée moyenne	23 h
Période	12/2025 – 09/2026
France compétences	96 %
Reste à charge titulaire	4 %

Formations engagées via le CPF — Caisse des Dépôts (open data), tous organismes confondus.