CERTIFICATION PROFESSIONNELLE

Expert réseaux infrastructures et sécuri

Code de la fiche : **RNCP39781**

Etat : **Active**

Télécharger la fiche | Aide en ligne | Supplément Europass : FR - EN

L'essentiel

Nomenclature du niveau de qualification	**Niveau 7**
Code(s) NSF	**326 :** Informatique, traitement de l'information, réseaux de transmission **326n :** Analyse informatique, conception d'architecture de réseaux
Formacode(s)	**24273 :** Architecture réseau **31094 :** Gestion projet informatique **31006 :** Sécurité informatique **31034 :** Administration système
Date d'échéance de l'enregistrement	**31-10-2029**

Certificateur(s)

Nom légal	Siret	Nom commercial	Site internet
ASSOCIATION POUR LA GESTION DE 3IL	39770462800015	Groupe 3iL	https://www.3il-ingenieurs.fr/

Résumé de la certification

Objectifs et contexte de la certification :

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)

Modalités d'évaluation :

Modalités d'évaluation par voie d'accès de la formation : Mises en situations professionnelles écrites, orales ou sur machine spécifiques pour chacun des 4 blocs + évaluation complémentaire post-blocs d'un Projet d'Étude Professionnel.

Modalités d'évaluation par voie d'accès de la VAE : Élaboration d'un dossier de validation et entretien avec un jury.

Blocs de compétences

RNCP39781BC01 - Gouverner les Infrastructures Systèmes et Réseaux

Liste de compétences	Modalités d'évaluation
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	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	Modalités d'évaluation
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	Mise en situation professionnelle simulée de montage d'infrastructure Mise en situation professionnelle – étude de cas sur l'organisation de la

Liste de compétences	Modalités d'évaluation
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	gestion des incidents et du support

RNCP39781BC03 - Piloter la Sécurité des Systèmes d'Information

Liste de compétences	Modalités d'évaluation
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	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	Modalités d'évaluation
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 (COPIL, 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)	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

Description des modalités d'acquisition de la certification par capitalisation des blocs de compétences et/ou par correspondance :

Voie d'accès à la certification par la formation : Validation des 4 blocs de compétences par leurs modalités d'évaluations spécifiques et évaluation complémentaire (soutenance orale portant sur une période d'application pratique en entreprise d'au moins 3 mois évaluée par un jury de professionnels).

Voie d'accès à la certification par la VAE : Validation de l'ensemble des blocs de compétences par un dossier de valorisation et entretien devant un jury VAE.

L'accès à la certification professionnelle est également possible par la mise en œuvre d'un parcours mixte (formation + VAE).

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

Code(s) ROME :

M1801 - Administration de systèmes d''information

M1802 - Expertise et support en systèmes d''information

M1803 - Direction des systèmes d''information

M1806 - Conseil et maîtrise d''ouvrage en systèmes d''information

M1810 - Production et exploitation de systèmes d''information

Références juridiques des 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.

Voie d’accès

Le cas échant, 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.

Le cas échant, prérequis à la validation de la certification :

Pré-requis disctincts pour les blocs de compétences :

Non

Voie d’accès à la certification	Oui	Non	Composition des jurys	Date de dernière modification
Après un parcours de formation sous statut d’élève ou d’étudiant	X		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	31-10-2024
En contrat d’apprentissage	X		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	31-10-2024

Voie d'accès à la certification	Oui	Non	Composition des jurys	Date de dernière modification
Après un parcours de formation continue	X		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	31-10-2024
En contrat de professionnalisation	X		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	31-10-2024
Par candidature individuelle		X	-	-
Par expérience	X		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	31-10-2024

	Oui	Non
Inscrite au cadre de la Nouvelle Calédonie		X
Inscrite au cadre de la Polynésie française		X

Liens avec d'autres certifications professionnelles, certifications ou habilitations

Certifications professionnelles enregistrées au RNCP en correspondance partielle :

Bloc(s) de compétences concernés	Code et intitulé de la certification professionnelle reconnue en correspondance partielle	Bloc(s) de compétences en correspondance partielle
RNCP39781BC01 - Gouverner les Infrastructures Systèmes et Réseaux	**RNCP38117 - Ingénieur systèmes, réseaux et cybersécurité**	RNCP38117BC04 - MANAGER LA PERFORMANCE DES SYSTEMES ET RESEAUX D'UNE ORGANISATION
RNCP39781BC01 - Gouverner les Infrastructures Systèmes et Réseaux **ET** RNCP39781BC03 - Piloter la	**RNCP38105 - Ingénieur systèmes, réseaux et cybersécurité**	RNCP38105BC04 - Maintenir le système en condition opérationnelle et de sécurité

Bloc(s) de compétences concernés	Code et intitulé de la certification professionnelle reconnue en correspondance partielle	Bloc(s) de compétences en correspondance partielle
Sécurité des Systèmes d'Information		
RNCP39781BC02 - Concevoir et Piloter les Infrastructures Systèmes et Réseaux	**RNCP36296 - Expert en architectures systèmes-réseaux et en sécurité informatique**	RNCP36296BC01 - Analyser et concevoir les infrastructures répondant à des besoins identifiés. **ET** RNCP36296BC03 - Superviser le déploiement et l'amélioration des infrastructures.
RNCP39781BC02 - Concevoir et Piloter les Infrastructures Systèmes et Réseaux	**RNCP38105 - Ingénieur systèmes, réseaux et cybersécurité**	RNCP38105BC03 - Concevoir l'architecture, réaliser et déployer la solution technique
RNCP39781BC02 - Concevoir et Piloter les Infrastructures Systèmes et Réseaux	**RNCP38117 - Ingénieur systèmes, réseaux et cybersécurité**	RNCP38117BC01 - PILOTER LA CONCEPTION D'UNE INFRASTRUCTURE SYSTEMES, RESEAUX SECURISEE ET RESPECTUEUSE DE LA POLITIQUE RSE D'UNE ORGANISATION **ET** RNCP38117BC02 - SUIVRE ET METTRE EN ŒUVRE LE DEPLOIEMENT DE L'INFRASTRUCTURE SYSTEMES ET RESEAUX SECURISEE ADAPTEE AUX BESOINS
RNCP39781BC02 - Concevoir et Piloter les Infrastructures Systèmes et Réseaux	**RNCP38823 - Expert en architectures systèmes, réseaux et sécurité informatique**	RNCP38823BC02 - Développer des solutions d'infrastructure systèmes et réseaux
RNCP39781BC02 - Concevoir et Piloter les Infrastructures Systèmes et Réseaux **ET** RNCP39781BC04 - Piloter les Projets et la Conduite du Changement	**RNCP38823 - Expert en architectures systèmes, réseaux et sécurité informatique**	RNCP38823BC01 - Planifier et organiser un projet d'architecture systèmes et réseaux
RNCP39781BC03 - Piloter la Sécurité des Systèmes d'Information	**RNCP36296 - Expert en architectures systèmes-réseaux et en sécurité informatique**	RNCP36296BC04 - Identifier les risques et définir la politique de sécurité du système d'information.
RNCP39781BC03 - Piloter la Sécurité des Systèmes d'Information	**RNCP38117 - Ingénieur systèmes, réseaux et cybersécurité**	RNCP38117BC03 - ELABORER LA STRATEGIE DE SECURISATION DE L'INFRASTRUCTURE INFORMATIQUE
RNCP39781BC03 - Piloter la Sécurité des Systèmes d'Information	**RNCP38779 - Manager en infrastructures et cybersécurité des systèmes d'information**	RNCP38779BC04 - Sécuriser les infrastructures du système d'Information (accès, réseaux et données)
RNCP39781BC03 - Piloter la Sécurité des Systèmes d'Information	**RNCP38823 - Expert en architectures systèmes, réseaux et sécurité informatique**	RNCP38823BC03 - Piloter la sécurité de l'infrastructure informatique

Bloc(s) de compétences concernés	Code et intitulé de la certification professionnelle reconnue en correspondance partielle	Bloc(s) de compétences en correspondance partielle
RNCP39781BC04 - Piloter les Projets et la Conduite du Changement	**RNCP36296 - Expert en architectures systèmes-réseaux et en sécurité informatique**	RNCP36296BC02 - Manager les projets du système d'information
RNCP39781BC04 - Piloter les Projets et la Conduite du Changement	**RNCP38105 - Ingénieur systèmes, réseaux et cybersécurité**	RNCP38105BC01 - Gérer un projet international **ET** RNCP38105BC02 - Recueillir et analyser les exigences du client
RNCP39781BC04 - Piloter les Projets et la Conduite du Changement	**RNCP38117 - Ingénieur systèmes, réseaux et cybersécurité**	RNCP38117BC05 - ELABORER UNE STRATEGIE DE GESTION DES NOUVEAUX PROJETS INFORMATIQUES D'UNE ORGANISATION
RNCP39781BC04 - Piloter les Projets et la Conduite du Changement	**RNCP38779 - Manager en infrastructures et cybersécurité des systèmes d'information**	RNCP38779BC01 - Manager les équipes et la transformation du SI **ET** RNCP38779BC02 - Superviser le portefeuille projets de la DSI et sa mise en œuvre
RNCP39781BC04 - Piloter les Projets et la Conduite du Changement	**RNCP38823 - Expert en architectures systèmes, réseaux et sécurité informatique**	RNCP38823BC04 - Piloter l'équipe du projet d'architecture informatique

Anciennes versions de la certification professionnelle reconnues en correspondance partielle :

Bloc(s) de compétences concernés	Code et intitulé de la certification professionnelle reconnue en correspondance partielle	Bloc(s) de compétences en correspondance partielle
RNCP39781BC01 - Gouverner les Infrastructures Systèmes et Réseaux	**RNCP34407 - Expert réseaux infrastructures et sécurité**	RNCP34407BC03 - Mettre en production et maintenir un système d'informations
RNCP39781BC02 - Concevoir et Piloter les Infrastructures Systèmes et Réseaux	**RNCP34407 - Expert réseaux infrastructures et sécurité**	RNCP34407BC04 - Administration de systèmes et réseaux informatiques
RNCP39781BC03 - Piloter la Sécurité des Systèmes d'Information	**RNCP34407 - Expert réseaux infrastructures et sécurité**	RNCP34407BC05 - Prévention Cyber Sécurité
RNCP39781BC04 - Piloter les Projets et la Conduite du Changement	**RNCP34407 - Expert réseaux infrastructures et sécurité**	RNCP34407BC01 - Piloter la maîtrise d'ouvrage d'un projet inforormatique **ET** RNCP34407BC02 - Mettre en oeuvre un projet informatique

Base légale

Référence au(x) texte(s) règlementaire(s) instaurant la certification :

Date du JO/BO	Référence au JO/BO
14/04/2012	Arrêté du 5 avril 2012 publié au Journal Officiel du 14 avril 2012 portant enregistrement au répertoire national des certifications professionnelles. Enregistrement pour trois ans, au niveau I, sous l'intitulé " Manager de systèmes d'information et d'infrastructure" avec effet au 02 janvier 2006 jusqu'au 7 août 2015

Référence des arrêtés et décisions publiés au Journal Officiel ou au Bulletin Officiel (enregistrement au RNCP, création diplôme, accréditation...) :

Date du JO/BO	Référence au JO/BO
17/03/2016	Arrêté du 25 février 2016 publié au Journal Officiel du 17 mars 2016 portant enregistrement au répertoire national des certifications professionnelles. Enregistrement pour deux ans, au niveau I, sous l'intitulé "Manager de systèmes d'information et d'infrastructure" avec effet au 7 août 2015, jusqu'au 17 mars 2018
27/01/2020	Date de décision : 27/01/2020 – Durée de l'enregistrement : 5 ans - Date d'échéance de l'enregistrement : 27/01/2025

Date du dernier Journal Officiel ou Bulletin Officiel :

27-01-2020

Date de décision	31-10-2024
Durée de l'enregistrement en années	5
Date d'échéance de l'enregistrement	31-10-2029
Date de dernière délivrance possible de la certification	31-10-2033

Pour plus d'informations

Statistiques :

Année d'obtention de la certification	Nombre de certifiés	Nombre de certifiés à la suite d'un parcours vae	Taux d'insertion global à 6 mois (en %)	Taux d'insertion dans le métier visé à 6 mois (en %)	Taux d'insertion dans le métier visé à 2 ans (en %)
2022	100	1	96	78	86
2021	41	3	97	51	74
2020	37	0	83	60	75

Lien internet vers le descriptif de la certification :

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

Liste des organismes préparant à la certification :

Liste des organismes préparant à la certification

Certification(s) antérieure(s) :

Code de la fiche	Intitulé de la certification remplacée
RNCP34407	Expert réseaux infrastructures et sécurité

Référentiel d'activité, de compétences et d'évaluation :

Référentiel d'activité, de compétences et d'évaluation