

Administrateur systèmes, réseaux et sécurité des infrastructures IT/OT

RNCP42829 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Code(s) NSF	200, 326, 326n
Formacode(s)	24220, 31006, 31032, 24426
Code(s) ROME	M1801
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	30/09/2026
Date d'échéance	30/09/2029

Certificateur(s)

AFORP FORMATION (CFAI) · SIRET : 77572845400205

Partenaires habilités

2 organismes habilités, d'après la liste publiée par France compétences : 2 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
ASS PROMOTION APPRENTISSAGE INDUSTRIES	39279259400039	Former et organiser l'évaluation
CFAI REGION NORD PAS-DE-CALAIS	30048880600120	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

La transformation numérique des organisations s'accompagne d'une hybridation croissante des infrastructures informatiques (IT) et industrielles (OT). Les systèmes d'information traditionnels interagissent désormais avec des systèmes industriels, des équipements connectés, des automates, des réseaux de capteurs et des environnements de production, notamment dans les secteurs de l'industrie, de l'énergie, des transports, du bâtiment et des services critiques.

Cette convergence IT/OT s'accompagne: D'une augmentation des exigences de disponibilité, de continuité de service et de sécurité ; D'une exposition accrue aux risques cyber, en particulier sur des infrastructures historiquement peu conçues pour être connectées ; D'un renforcement des exigences réglementaires et normatives (cybersécurité, protection des données, continuité d'activité, exigences sectorielles).

Dans ce contexte, les organisations expriment un besoin croissant de professionnels opérationnels capables d'administrer, d'exploiter et de sécuriser des infrastructures hybrides IT/OT, sans pour autant relever d'un rôle d'expert ou d'architecte de haut niveau.

Le marché de l'emploi fait apparaître une tension durable sur les métiers de l'administration des systèmes, réseaux et infrastructures, renforcée par : La complexification des environnements techniques ; La multiplication des incidents de sécurité ; L'intégration progressive des environnements industriels aux systèmes d'information. Les employeurs recherchent des profils capables de : Administrer des infrastructures systèmes et réseaux complexes ; Assurer la sécurité opérationnelle des environnements IT ; Prendre en compte les spécificités des environnements OT (contraintes industrielles, protocoles, continuité de production, sécurité adaptée) ; Maintenir les infrastructures en conditions opérationnelles, tout en respectant les exigences de sécurité et de conformité.

La certification répond à ce besoin en formant des administrateurs systèmes, réseaux et sécurité disposant d'une compréhension opérationnelle des infrastructures IT/OT, aptes à intervenir sur des environnements hybrides. Elle a pour objectif de valider les compétences nécessaires pour : Administrer et exploiter des infrastructures systèmes et réseaux, incluant serveurs, réseaux, environnements virtualisés, services et équipements connectés ; Assurer la sécurité opérationnelle des infrastructures, par la mise en œuvre de configurations sécurisées, la gestion des accès, la supervision et la gestion des incidents ; Intervenir sur des environnements hybrides IT/OT, en tenant compte des contraintes spécifiques des systèmes industriels (disponibilité, sûreté, protocoles, segmentation) ; Maintenir les infrastructures en conditions opérationnelles, en assurant la supervision, la maintenance, la gestion des évolutions et la continuité de service ; Appliquer les bonnes pratiques professionnelles, réglementaires et organisationnelles liées à la cybersécurité et à l'exploitation des infrastructures.

Le professionnel certifié exerce un rôle opérationnel d'administrateur, intervenant sur l'exploitation, la sécurité et la supervision des infrastructures informatiques et industrielles. Il ne s'agit ni d'un expert en cybersécurité stratégique, ni d'un architecte d'infrastructures complexes, mais d'un administrateur confirmé capable : De mettre en œuvre des solutions définies ; D'exploiter et sécuriser des environnements existants ; D'interagir avec des experts, ingénieurs ou prestataires spécialisés le cas échéant.

ACTIVITÉS VISÉES

Le titulaire de la certification exerce des activités d'administration, d'exploitation et de sécurisation d'infrastructures informatiques et industrielles, au sein d'environnements hybrides IT/OT.

Il intervient principalement sur des infrastructures existantes, en garantissant leur fonctionnement, leur sécurité et leur disponibilité.

Ses principales activités sont : Analyser l'existant des infrastructures systèmes et réseaux IT ; Administrer les systèmes et les environnements serveurs ; Administrer les services réseaux et d'infrastructure IT ; Gérer les utilisateurs, les droits et les accès ; Exploiter et maintenir les infrastructures systèmes et réseaux IT ; Diagnostiquer et résoudre les incidents systèmes et réseaux ; Documenter et communiquer sur l'infrastructure IT ; Analyser et appréhender les environnements hybrides IT/OT ; Administrer les infrastructures hybrides IT/OT ; Superviser les infrastructures hybrides IT/OT ; Intervenir sur les incidents des environnements hybrides IT/OT ; Documenter et communiquer sur les environnements hybrides IT/OT ; Analyser les risques et le niveau de sécurité des infrastructures IT et IT/OT ; Mettre en œuvre les mesures de sécurité opérationnelle ; Surveiller et détecter les événements de sécurité ; Intervenir sur les incidents de sécurité IT et IT/OT ; Maintenir et améliorer la sécurité opérationnelle ; Superviser durablement les infrastructures IT et IT/OT ; Maintenir les infrastructures IT et IT/OT en conditions opérationnelles ; Améliorer en continu les infrastructures IT et IT/OT ; Intégrer les enjeux de durabilité et de responsabilité dans l'exploitation des infrastructures ; Assurer une veille technique et professionnelle ; Documenter et communiquer dans une logique d'amélioration continue.

COMPÉTENCES ATTESTÉES

Analyser une infrastructure systèmes et réseaux IT existante, à partir d'éléments techniques et organisationnels, en identifiant ses architectures, composants, services, flux et dépendances, afin de diagnostiquer son état de fonctionnement et d'identifier les points critiques impactant la disponibilité, la performance et la continuité d'exploitation.

Administrer des systèmes et des environnements serveurs, en installant, configurant et supervisant des systèmes d'exploitation et des services associés, en gérant des environnements virtualisés et/ou conteneurisés et en arbitrant des choix techniques d'architecture ou d'évolution, afin d'assurer la stabilité, la disponibilité et la cohérence des systèmes dans le respect des contraintes d'exploitation.

Administrer des services réseaux et d'infrastructure IT, en déployant et configurant les services réseaux essentiels, l'adressage IP, le routage et les interconnexions, et en adaptant les configurations aux contraintes d'exploitation, afin d'assurer la connectivité, la disponibilité et la continuité de service des infrastructures IT.

Gérer les utilisateurs, les droits et les accès, en administrant les comptes, groupes et habilitations aux ressources systèmes et réseaux, en contrôlant leur conformité aux règles définies par l'organisation, afin de garantir un accès sécurisé et adapté aux besoins opérationnels.

Exploiter et maintenir des infrastructures systèmes et réseaux IT, en mettant en œuvre les procédures d'exploitation, de maintenance, de sauvegarde et de restauration, en supervisant leur fonctionnement et en planifiant les interventions techniques, afin d'assurer la disponibilité, la fiabilité et la continuité de service dans le respect des contraintes d'exploitation.

Diagnostiquer et résoudre des incidents systèmes et réseaux, en appliquant une méthodologie structurée d'analyse des dysfonctionnements, en priorisant les actions correctives et en assurant la traçabilité des interventions, afin de

rétablir le fonctionnement normal des services dans le respect des engagements de service.

Documenter et communiquer sur une infrastructure IT, en produisant et en mettant à jour une documentation technique et opérationnelle structurée et en formalisant les procédures d'exploitation et d'intervention, afin de garantir la compréhension, la traçabilité et la maintenabilité de l'infrastructure par les parties prenantes.

Analyser un environnement hybride IT/OT, en identifiant les architectures, composants IT et OT, interfaces et flux d'interconnexion, en évaluant les impacts techniques et opérationnels des interactions IT/OT, afin de diagnostiquer le fonctionnement global de l'infrastructure et les contraintes de continuité, de sûreté et d'exploitation propres aux environnements industriels.

Administrer des infrastructures hybrides IT/OT, en configurant et en maintenant les systèmes et réseaux participant à l'interconnexion, en mettant en œuvre des mécanismes de segmentation et de cloisonnement et en coordonnant les interventions entre acteurs IT et OT, afin d'assurer la disponibilité, la cohérence et la continuité des environnements hybrides dans le respect des contraintes industrielles.

Superviser des infrastructures hybrides IT/OT, en mettant en œuvre et en exploitant des dispositifs de supervision adaptés, en analysant et en priorisant les alertes et événements détectés, afin d'identifier les anomalies susceptibles d'affecter la disponibilité et la continuité des environnements industriels.

Intervenir sur des incidents affectant des environnements hybrides IT/OT, en appliquant une méthodologie structurée d'analyse des dysfonctionnements, en coordonnant et en priorisant les actions de résolution avec les parties prenantes IT et OT, et en assurant la traçabilité des interventions, afin de rétablir les services en limitant les impacts sur les processus industriels.

Documenter et communiquer sur des environnements hybrides IT/OT, en produisant et en mettant à jour une documentation technique et opérationnelle structurée, en formalisant les procédures d'exploitation et d'intervention spécifiques et en assurant la coordination des informations entre acteurs IT et OT, afin de garantir la compréhension, la traçabilité et la continuité d'exploitation des environnements hybrides.

Analyser le niveau de sécurité d'infrastructures IT et IT/OT, en identifiant et en priorisant les vulnérabilités techniques et organisationnelles ainsi que les risques opérationnels associés, afin d'évaluer l'exposition des systèmes au regard des contraintes d'exploitation, de continuité de service et, le cas échéant, des exigences industrielles.

Mettre en œuvre des mesures de sécurité opérationnelle sur des infrastructures IT et IT/OT, en déployant, configurant et maintenant les mécanismes de sécurité définis par l'organisation, en vérifiant leur efficacité et en assurant la traçabilité des actions réalisées, afin de réduire l'exposition aux risques tout en respectant les contraintes d'exploitation.

Surveiller la sécurité d'infrastructures IT et IT/OT, en exploitant et en analysant les journaux, alertes et événements issus des dispositifs de surveillance, en qualifiant et en priorisant les incidents détectés, afin d'anticiper et de limiter les impacts sur les systèmes et les processus industriels.

Intervenir sur des incidents de sécurité affectant des infrastructures IT et IT/OT, en appliquant une méthodologie structurée d'analyse, en priorisant les actions de réponse et de remédiation et en assurant la traçabilité des interventions, afin de limiter les impacts sur les systèmes et les processus industriels et de rétablir un état sécurisé.

Maintenir et améliorer la sécurité opérationnelle d'infrastructures IT et IT/OT, en mettant à jour les configurations et dispositifs de sécurité, en capitalisant sur les incidents rencontrés et en appliquant un cadre méthodologique structuré d'analyse et de gestion des incidents, afin de renforcer durablement le niveau de sécurité et d'assurer la cohérence et la traçabilité des actions menées.

Superviser durablement des infrastructures IT et IT/OT en conditions opérationnelles, en analysant et en exploitant les indicateurs de performance, de disponibilité et de qualité de service, en adaptant les indicateurs si nécessaire et en proposant des actions d'amélioration fondées sur les données de supervision, afin d'assurer le pilotage opérationnel et la maîtrise des dérives.

Maintenir des infrastructures IT et IT/OT en conditions opérationnelles, en planifiant, priorisant et réalisant les actions de maintenance préventive et corrective, en arbitrant les évolutions techniques au regard des risques et des contraintes d'exploitation, afin d'assurer la continuité et la stabilité des services dans la durée.

Améliorer en continu des infrastructures IT et IT/OT, en proposant, argumentant et mettant en œuvre des actions d'optimisation fondées sur l'analyse des incidents, des retours d'expérience et des indicateurs de performance, en priorisant les actions au regard des enjeux techniques, organisationnels et économiques, afin d'accroître durablement la performance, la fiabilité et la maintenabilité des infrastructures.

Intégrer les enjeux de durabilité et de responsabilité dans l'exploitation d'infrastructures IT et IT/OT, en mettant en œuvre des actions concrètes d'optimisation des ressources, de rationalisation des services et de gestion du cycle de vie des équipements, en arbitrant les choix techniques au regard de leur impact environnemental et opérationnel, afin de concilier performance, continuité de service et réduction de l'empreinte environnementale.

Assurer une veille technique et professionnelle sur les infrastructures IT et IT/OT, en identifiant et en exploitant des sources documentaires spécialisées, y compris en langue anglaise, en analysant de manière critique les évolutions identifiées et en formalisant leur impact potentiel, afin d'anticiper les adaptations nécessaires des infrastructures exploitées.

Documenter et communiquer sur les infrastructures IT et IT/OT dans une logique d'amélioration continue, en mettant à jour et en structurant la documentation technique et opérationnelle, en formalisant les évolutions, retours d'expérience et bonnes pratiques, afin d'assurer la capitalisation des connaissances, la traçabilité des évolutions et la coordination entre les parties prenantes.

Blocs de compétences

RNCP42829BC01 — Administrer et exploiter des infrastructures systèmes et réseaux IT

LISTE DE COMPÉTENCES

Analyser une infrastructure systèmes et réseaux IT existante, à partir d'éléments techniques et organisationnels, en identifiant ses architectures, composants, services, flux et dépendances, afin de diagnostiquer son état de fonctionnement et d'identifier les points critiques impactant la disponibilité, la performance et la continuité d'exploitation.

Administrer des systèmes et des environnements serveurs, en installant, configurant et supervisant des systèmes d'exploitation et des services associés, en gérant des environnements virtualisés et/ou conteneurisés et en arbitrant des choix techniques d'architecture ou d'évolution, afin d'assurer la stabilité, la disponibilité et la cohérence des systèmes dans le respect des contraintes d'exploitation.

Administrer des services réseaux et d'infrastructure IT, en déployant et configurant les services réseaux essentiels, l'adressage IP, le routage et les interconnexions, et en adaptant les configurations aux contraintes d'exploitation, afin d'assurer la connectivité, la disponibilité et la continuité de service des infrastructures IT.

Gérer les utilisateurs, les droits et les accès, en administrant les comptes, groupes et habilitations aux ressources systèmes et réseaux, en contrôlant leur conformité aux règles définies par l'organisation, afin de garantir un accès sécurisé et adapté aux besoins opérationnels.

Exploiter et maintenir des infrastructures systèmes et réseaux IT, en mettant en œuvre les procédures d'exploitation, de maintenance, de sauvegarde et de restauration, en supervisant leur fonctionnement et en planifiant les interventions techniques, afin d'assurer la disponibilité, la fiabilité et la continuité de service dans le respect des contraintes d'exploitation.

Diagnostiquer et résoudre des incidents systèmes et réseaux, en appliquant une méthodologie structurée d'analyse des dysfonctionnements, en priorisant les actions correctives et en assurant la traçabilité des interventions, afin de rétablir le fonctionnement normal des services dans le respect des engagements de service.

Documenter et communiquer sur une infrastructure IT, en produisant et en mettant à jour une documentation technique et opérationnelle structurée et en formalisant les procédures d'exploitation et d'intervention, afin de garantir la compréhension, la traçabilité et la maintenabilité de l'infrastructure par les parties prenantes.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle individuelle, réalisée sur une infrastructure réelle ou reconstituée comprenant : Des serveurs physiques ou virtualisés ; Des équipements réseau ; Des services d'infrastructure ; Des incidents ou anomalies simulés

Le candidat doit : Analyser l'environnement existant ; Mettre en œuvre des actions d'administration et de configuration ; Gérer des droits et des accès ; Réaliser des opérations d'exploitation et de maintenance ; Diagnostiquer et résoudre un incident ; Produire une documentation associée.

Les livrables attendus comprennent : Une cartographie d'infrastructure ; Les configurations réalisées ; Un compte rendu d'intervention ; Les procédures mises à jour ; Un rapport de diagnostic d'incident.

Une soutenance orale permet d'évaluer la justification des choix techniques, la méthodologie employée et la capacité d'explicitation.

L'évaluation s'appuie sur une grille critériée permettant de statuer sur l'acquisition des compétences du bloc.

RNCP42829BC02 — Administrer et superviser des infrastructures hybrides IT/OT

LISTE DE COMPÉTENCES

Analyser un environnement hybride IT/OT, en identifiant les architectures, composants IT et OT, interfaces et flux d'interconnexion, en évaluant les impacts techniques et opérationnels des interactions IT/OT, afin de diagnostiquer le

fonctionnement global de l'infrastructure et les contraintes de continuité, de sûreté et d'exploitation propres aux environnements industriels.

Administrer des infrastructures hybrides IT/OT, en configurant et en maintenant les systèmes et réseaux participant à l'interconnexion, en mettant en œuvre des mécanismes de segmentation et de cloisonnement et en coordonnant les interventions entre acteurs IT et OT, afin d'assurer la disponibilité, la cohérence et la continuité des environnements hybrides dans le respect des contraintes industrielles.

Superviser des infrastructures hybrides IT/OT, en mettant en œuvre et en exploitant des dispositifs de supervision adaptés, en analysant et en priorisant les alertes et événements détectés, afin d'identifier les anomalies susceptibles d'affecter la disponibilité et la continuité des environnements industriels.

Intervenir sur des incidents affectant des environnements hybrides IT/OT, en appliquant une méthodologie structurée d'analyse des dysfonctionnements, en coordonnant et en priorisant les actions de résolution avec les parties prenantes IT et OT, et en assurant la traçabilité des interventions, afin de rétablir les services en limitant les impacts sur les processus industriels.

Documenter et communiquer sur des environnements hybrides IT/OT, en produisant et en mettant à jour une documentation technique et opérationnelle structurée, en formalisant les procédures d'exploitation et d'intervention spécifiques et en assurant la coordination des informations entre acteurs IT et OT, afin de garantir la compréhension, la traçabilité et la continuité d'exploitation des environnements hybrides.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle individuelle, réalisée sur une infrastructure hybride IT/OT réelle ou reconstituée comprenant : • Des serveurs et services d'infrastructure IT ; Des équipements réseau IT et des mécanismes d'interconnexion ; Des composants OT (automates, systèmes de supervision, réseaux industriels ou maquettes représentatives) ; • Des flux et interfaces entre environnements IT et OT ; Des incidents ou anomalies simulés affectant les interactions IT/OT

Le candidat doit : Analyser l'architecture hybride IT/OT existante ; Identifier les composants, flux et interconnexions entre environnements IT et OT ; Administrer les systèmes et réseaux participant à l'interconnexion IT/OT ; Mettre en œuvre ou maintenir des mécanismes de segmentation et de cloisonnement ; Superviser le fonctionnement des environnements hybrides ; Intervenir sur un incident affectant les interactions IT/OT ; Produire une documentation associée

Les livrables attendus comprennent : Une analyse documentée de l'architecture hybride IT/OT ; Une cartographie des flux et interconnexions ; Les configurations réalisées ou modifiées ; Un compte rendu d'intervention sur incident IT/OT ; Les procédures d'exploitation ou de coordination mises à jour ; Un rapport argumenté présentant les choix techniques réalisés et la prise en compte des contraintes industrielles

Une soutenance orale permet d'évaluer la justification des choix techniques, la compréhension des interactions IT/OT, la prise en compte des contraintes de continuité et de sûreté, ainsi que la capacité à expliciter les impacts des actions menées sur les environnements industriels.

L'évaluation s'appuie sur une grille critériée permettant de statuer sur l'acquisition des compétences du bloc.

RNCP42829BC03 — Assurer la sécurité opérationnelle des infrastructures IT et IT/OT

LISTE DE COMPÉTENCES

Analyser le niveau de sécurité d'infrastructures IT et IT/OT, en identifiant et en priorisant les vulnérabilités techniques et organisationnelles ainsi que les risques opérationnels associés, afin d'évaluer l'exposition des systèmes au regard des contraintes d'exploitation, de continuité de service et, le cas échéant, des exigences industrielles.

Mettre en œuvre des mesures de sécurité opérationnelle sur des infrastructures IT et IT/OT, en déployant, configurant et maintenant les mécanismes de sécurité définis par l'organisation, en vérifiant leur efficacité et en assurant la traçabilité des actions réalisées, afin de réduire l'exposition aux risques tout en respectant les contraintes d'exploitation.

Surveiller la sécurité d'infrastructures IT et IT/OT, en exploitant et en analysant les journaux, alertes et événements issus des dispositifs de surveillance, en qualifiant et en priorisant les incidents détectés, afin d'anticiper et de limiter les impacts sur les systèmes et les processus industriels.

Intervenir sur des incidents de sécurité affectant des infrastructures IT et IT/OT, en appliquant une méthodologie structurée d'analyse, en priorisant les actions de réponse et de remédiation et en assurant la traçabilité des interventions, afin de limiter les impacts sur les systèmes et les processus industriels et de rétablir un état sécurisé.

Maintenir et améliorer la sécurité opérationnelle d'infrastructures IT et IT/OT, en mettant à jour les configurations et dispositifs de sécurité, en capitalisant sur les incidents rencontrés et en appliquant un cadre méthodologique structuré d'analyse et de gestion des incidents, afin de renforcer durablement le niveau de sécurité et d'assurer la cohérence et

la traçabilité des actions menées.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle individuelle, réalisée sur une infrastructure IT et/ou IT/OT réelle ou reconstituée comprenant : Des serveurs, équipements réseau et services d'infrastructure ; Des composants éventuellement intégrés à un environnement hybride IT/OT ; Des dispositifs de sécurité (pare-feu, mécanismes de filtrage, outils de supervision ou équivalents) ; Des vulnérabilités ou incidents de sécurité simulés

Le candidat doit : Analyser le niveau de sécurité de l'infrastructure ; Identifier et prioriser les vulnérabilités techniques et organisationnelles ; Mettre en œuvre des mesures de sécurité opérationnelle adaptées ; Surveiller les événements et alertes de sécurité ; Intervenir sur un incident de sécurité simulé ; Documenter les actions réalisées et les mesures mises en œuvre

Les livrables attendus comprennent : Une analyse documentée du niveau de sécurité ; Une priorisation des vulnérabilités identifiées ; Les configurations ou mesures de sécurité mises en œuvre ; Un compte rendu d'incident de sécurité ; Les procédures ou dispositifs de sécurité mis à jour ; Un rapport argumenté justifiant les choix techniques réalisés

Une soutenance orale permet d'évaluer : La justification des mesures de sécurité mises en œuvre ; La capacité à analyser les risques au regard des contraintes d'exploitation ; La cohérence des actions de surveillance et de remédiation ; La prise en compte des impacts sur la continuité de service et, le cas échéant, sur les environnements industriels

L'évaluation s'appuie sur une grille critériée permettant de statuer sur l'acquisition des compétences du bloc.

RNCP42829BC04 — Maintenir, superviser et améliorer les infrastructures IT et IT/OT en conditions opérationnelles

LISTE DE COMPÉTENCES

Superviser durablement des infrastructures IT et IT/OT en conditions opérationnelles, en analysant et en exploitant les indicateurs de performance, de disponibilité et de qualité de service, en adaptant les indicateurs si nécessaire et en proposant des actions d'amélioration fondées sur les données de supervision, afin d'assurer le pilotage opérationnel et la maîtrise des dérives.

Maintenir des infrastructures IT et IT/OT en conditions opérationnelles, en planifiant, priorisant et réalisant les actions de maintenance préventive et corrective, en arbitrant les évolutions techniques au regard des risques et des contraintes d'exploitation, afin d'assurer la continuité et la stabilité des services dans la durée.

Améliorer en continu des infrastructures IT et IT/OT, en proposant, argumentant et mettant en œuvre des actions d'optimisation fondées sur l'analyse des incidents, des retours d'expérience et des indicateurs de performance, en priorisant les actions au regard des enjeux techniques, organisationnels et économiques, afin d'accroître durablement la performance, la fiabilité et la maintenabilité des infrastructures.

Intégrer les enjeux de durabilité et de responsabilité dans l'exploitation d'infrastructures IT et IT/OT, en mettant en œuvre des actions concrètes d'optimisation des ressources, de rationalisation des services et de gestion du cycle de vie des équipements, en arbitrant les choix techniques au regard de leur impact environnemental et opérationnel, afin de concilier performance, continuité de service et réduction de l'empreinte environnementale.

Assurer une veille technique et professionnelle sur les infrastructures IT et IT/OT, en identifiant et en exploitant des sources documentaires spécialisées, y compris en langue anglaise, en analysant de manière critique les évolutions identifiées et en formalisant leur impact potentiel, afin d'anticiper les adaptations nécessaires des infrastructures exploitées.

Documenter et communiquer sur les infrastructures IT et IT/OT dans une logique d'amélioration continue, en mettant à jour et en structurant la documentation technique et opérationnelle, en formalisant les évolutions, retours d'expérience et bonnes pratiques, afin d'assurer la capitalisation des connaissances, la traçabilité des évolutions et la coordination entre les parties prenantes.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle individuelle, réalisée sur une infrastructure IT et/ou IT/OT réelle ou reconstituée comprenant : Des serveurs et services d'infrastructure ; Des équipements réseau et mécanismes d'interconnexion ; Des composants éventuellement intégrés à un environnement hybride IT/OT ; Des outils de supervision et d'analyse de performance ; Des contraintes d'exploitation et d'amélioration continue formalisées

Le candidat doit : Superviser le fonctionnement global de l'infrastructure ; Analyser les indicateurs de performance et de disponibilité ; Identifier les axes d'amélioration technique ou organisationnelle ; Proposer et mettre en œuvre des actions d'optimisation ; Planifier les évolutions ou interventions techniques ; Documenter les actions réalisées et les améliorations proposées

Les livrables attendus comprennent : Une analyse documentée des indicateurs de performance et de disponibilité ; Un diagnostic des points d'amélioration identifiés ; Les actions d'optimisation mises en œuvre ou proposées ; Un plan d'intervention ou d'évolution argumenté ; Les configurations ou procédures mises à jour ; Un rapport présentant les gains attendus ou constatés

Une soutenance orale permet d'évaluer : La capacité à analyser les données issues de la supervision ; La pertinence des propositions d'amélioration ; La justification des choix techniques réalisés ; La prise en compte des contraintes d'exploitation et, le cas échéant, industrielles

L'évaluation s'appuie sur une grille critériée permettant de statuer sur l'acquisition des compétences du bloc.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Les titulaires de la certification exercent leurs activités au sein : D'entreprises de services du numérique (ESN) et sociétés d'ingénierie informatique ; D'entreprises industrielles intégrant des infrastructures hybrides IT/OT (industrie manufacturière, énergie, transport, agroalimentaire, etc.) ; D'organisations publiques ou privées disposant d'infrastructures systèmes et réseaux critiques ; D'opérateurs d'importance vitale (OIV) ou d'organisations soumises à des exigences renforcées en matière de sécurité et de continuité de service ; De collectivités territoriales, établissements publics ou structures parapubliques ; De PME, ETI et grands groupes disposant d'infrastructures IT internalisées.

TYPE D'EMPLOIS ACCESSIBLES

Administrateur systèmes et réseaux ; Administrateur systèmes, réseaux et sécurité ; Administrateur infrastructures IT ; Administrateur infrastructures hybrides IT/OT ; Administrateur sécurité opérationnelle (IT / IT-OT) ; Exploitant infrastructures IT ; Responsable technique d'infrastructure (PME/ETI) ; Référent infrastructures et sécurité ; Coordinateur exploitation et maintenance des infrastructures IT/OT.

RÉGLEMENTATIONS D'ACTIVITÉ

Le métier visé par ce titre ne relève pas, en tant que tels, d'une activité réglementée au sens strict. Toutefois, il s'inscrit dans des environnements fortement encadrés par des exigences réglementaires, normatives et contractuelles, notamment en matière de sécurité des systèmes d'information, de protection des données, de continuité de service et, le cas échéant, de protection des infrastructures critiques. L'environnement réglementaire européen et national a connu une évolution significative ; ces évolutions accroissent la responsabilité opérationnelle des administrateurs systèmes, réseaux et sécurité, qui doivent intégrer les exigences réglementaires dans leurs pratiques d'exploitation et de sécurisation.

Les référentiels renouvelés intègrent ces dimensions dans les activités d'analyse des risques, de mise en œuvre des mesures de sécurité opérationnelle et de maintien en conditions de sécurité. Cependant si les activités sont exercées par ces administrateurs dans le respect des règles, procédures et politiques définies par l'organisation, elles s'effectuent sous la responsabilité de l'employeur ou du donneur d'ordre. Ainsi l'administrateur intervient sous la responsabilité hiérarchique de son employeur et ne porte pas la responsabilité juridique globale de la conformité réglementaire.

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

L'accès à la formation préparant à la certification est ouvert à des publics disposant de bases solides en informatique et réseaux, leur permettant de suivre un parcours de niveau 6.

Sont notamment concernés : Les titulaires d'une certification ou d'un diplôme de niveau 5 dans les domaines des systèmes et réseaux, de l'informatique, des réseaux et télécommunications, de la cybersécurité ; Ou les personnes justifiant d'une expérience professionnelle significative dans les métiers de l'informatique, des systèmes ou des réseaux.

L'admission peut être conditionnée à l'étude du dossier de candidature, un entretien de positionnement, et, le cas échéant, des tests permettant de vérifier l'adéquation du projet professionnel et du niveau du candidat avec les exigences de la certification.

Les candidats doivent disposer de connaissances de base en informatique, notamment dans les domaines suivants : Fonctionnement des systèmes d'exploitation (Windows ou Linux), notions de réseaux informatiques (adressage IP, services réseau), utilisation des outils informatiques et des environnements techniques.

Une appétence pour l'administration des systèmes, les infrastructures réseaux et la cybersécurité est attendue.

Des dispositifs d'accompagnement ou de remise à niveau peuvent être proposés afin de permettre l'entrée et la réussite dans le parcours.

PRÉREQUIS À LA VALIDATION

La validation de la certification « Administrateur systèmes, réseaux et sécurité des infrastructures IT/OT » est conditionnée à la validation de l'ensemble des blocs de compétences qui la composent.

Pour obtenir la certification complète, le candidat doit avoir validé l'intégralité des blocs de compétences constitutifs de la certification, par la voie de la formation, de la capitalisation ou de la VAE ; Avoir satisfait aux modalités d'évaluation définies pour chaque bloc de compétences ; Avoir présenté les livrables professionnels attendus et soutenu ses travaux devant un jury. Justifier d'un équivalent B1 du Cadre Européen de référence pour les langues (CECRL) en français et en anglais

Aucun autre prérequis spécifique (diplôme, certification externe, habilitation ou expérience minimale supplémentaire) n'est exigé pour la validation de la certification.

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

Le jury de certification est composé de cinq membres : un président et quatre membres décisionnaires. Le président est désigné par les membres du jury parmi eux, préalablement à l'ouverture des délibérations.

L'ensemble des membres du jury est constitué de professionnels experts du domaine des systèmes, réseaux et cybersécurité. Ils sont tous extérieurs à l'AFORP : ils n'interviennent ni dans la formation, ni dans l'accompagnement pédagogique, et n'encadrent aucun candidat préparant la 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	30/09/2033

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2025	69	0	100 %	—
2024	44	0	100 %	88 %
2023	42	0	100 %	96 %
2022	24	0	100 %	91 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP39851

CORRESPONDANCES (PAR BLOCS)

RNCP39851

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

Formation alternance Administrateur systèmes, réseaux et sécurité des infrastructures IT/OT - AFORP

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/42829/>