

CERTIFICATION PROFESSIONNELLE

Accueil > Trouver une certification > Répertoire national des certifications professionnelles > Administrateur systèmes, réseaux et cybersécurité

Administrateur systèmes, réseaux et cybersécurité

Code de la fiche :
RNCP40356

Etat :
Active

 Télécharger la fiche

 Aide en ligne

 Supplément Europass : FR - EN

L'essentiel

	Nomenclature du niveau de qualification	Niveau 6
	Code(s) NSF	326 : Informatique, traitement de l'information, réseaux de transmission
	Formacode(s)	31034 : Administration système 31032 : Système exploitation informatique 31006 : Sécurité informatique 24231 : Réseau informatique 31008 : Système information
	Date d'échéance de l'enregistrement	28-03-2030

Certificateur(s)

Nom légal	Siret	Nom commercial	Site internet
OPENCLASSROOMS	49386136300098	-	-



Résumé de la certification

Objectifs et contexte de la certification :

L'administrateur systèmes, réseaux et sécurité est responsable de la performance et de la sécurité du système d'information de l'entreprise pour laquelle il travaille. Il doit être en mesure d'identifier et de mettre en œuvre les solutions qui répondent aux besoins et aux contraintes du SI sous sa responsabilité. Il fait évoluer le SI en cohérence avec les évolutions du contexte sans transiger sur le niveau de performance et de sécurité requis. Il intervient pour cela sur toutes les étapes du cycle de vie du SI, de sa conception initiale à son amélioration continue : en passant par sa mise en production, son administration et sa maintenance au quotidien.

En fonction de son cadre d'intervention, il pourra être amené soit à concentrer ses activités sur un périmètre donné dont il deviendra spécialiste (réseaux, systèmes, etc.), soit à endosser plusieurs casquettes nécessitant une certaine polyvalence et par conséquent, des savoir-faire variés et moins spécialisés. Il est donc important qu'un administrateur réseaux, systèmes et sécurité sache agir sur toutes les couches et tout le cycle de vie du SI.

Pour réussir ses missions, l'administrateur systèmes, réseaux et sécurité doit s'appuyer sur de solides compétences techniques et posséder des savoir-être (compétences comportementales) pour collaborer au quotidien avec ses interlocuteurs.

Activités visées :

Veille informationnelle (principalement réglementaire technologique et sécurité)

Collecte et analyse des besoin

Recherche d'une solution technique

Conseil auprès des décideurs

Établissement / formalisation du plan projet

Conception des infrastructures systèmes / réseaux

Mise en place des infrastructures systèmes / réseaux

Gestion des accès aux ressources

Gestion des actifs informatiques et configuration, des mises à jour et des sauvegardes

Supervision du bon fonctionnement des infrastructures informatique

Surveillance du degré de sécurité des infrastructures informatiques

Compétences attestées :

Définir et mettre en place un système de veille automatisée ou non afin de repérer les évolutions en lien avec son activité (Information Technology / technologies de l'information)

Analyser les informations collectées afin d'identifier les opportunités (ex : nouvelles technologies, nouveaux services cloud) et les éventuelles menaces (ex : cybermenaces, mise en conformité nécessaire) Le cas échéant, les partager avec ses pairs (communauté / réseau) ou bien des collaborateurs au sein d'une organisation

Analyser, le cas échéant préciser / affiner, et formaliser les besoins informatiques, afin d'identifier les objectifs (résultats attendus) et les éventuelles contraintes techniques, matérielles, budgétaires et réglementaires

Identifier une solution en termes d'infrastructure informatique, adaptée et conforme aux besoins / contraintes, à l'aide d'une recherche ponctuelle ciblée ou bien à partir de la veille, et la représenter visuellement, à l'aide d'un outil de modélisation adapté, afin d'en illustrer son implémentation, ses actions et ses éventuels impacts / risques

Estimer les coûts associés (humains et matériels) à la solution technique afin de déterminer le budget nécessaire à sa mise en production et à son exploitation

Présenter la solution technique, expliquer / argumenter ses choix techniques / financiers auprès des décideurs dans un objectif de validation

Organiser (définir / planifier / attribuer) les tâches nécessaires à la conception et à la mise en production de la solution dans le système d'information en cohérence avec les contraintes de l'organisation (notamment un minimum d'impact sur la continuité du

service)

Définir / structurer / modéliser l'architecture technique de l'infrastructure cible, à l'aide d'un logiciel adapté, selon l'agencement des briques fonctionnelles (utilisateurs / données / traitements souhaités) et les critères fournis (performance, sécurité, évolutivité, etc), afin de définir l'organisation et les caractéristiques des équipements / composants et leurs interactions
Identifier les configurations à appliquer sur les équipements / composants de l'infrastructure cible, à partir des ressources adaptées (ex : documentation fournisseur) et selon le modèle d'architecture défini afin d'en disposer selon l'usage voulu

Créer un prototype ou bien une version pilote (une maquette test) de l'infrastructure système / réseau, à l'aide d'un outil de simulation adapté, afin de visualiser et de tester les équipements / composants, leurs interactions et les fonctionnalités associées
Valider ou non la mise en production selon les résultats

Identifier les règles de durcissement (suppression des services inutiles, forcer la robustesse des mots de passe, etc), à partir des guides externes (ANSSI, fournisseurs, etc), les adapter si besoin aux contraintes de l'organisation afin de sécuriser les infrastructures
Installer et effectuer les réglages (configurations / sécurisation) sur les équipements / composants réseaux / systèmes, quel que soit le type d'infrastructure et le mode de déploiement, dans le respect des règles de l'art et selon les caractéristiques techniques et fonctionnelles définies

Élaborer et mettre en œuvre une procédure de test afin de valider la conformité et la fonctionnalité de l'infrastructure déployée

Rédiger l'ensemble des procédures nécessaires à la mise en production / au déploiement de la solution
Former les utilisateurs ou bien communiquer les bonnes pratiques liées à l'utilisation d'un nouveau service afin d'accompagner le changement

Organiser / mettre à jour un annuaire des rôles / des autorisations associées à l'aide d'un outil adapté selon les droits définis, dans le respect de la politique de sécurité de l'organisation et de la réglementation en vigueur (sur les données) afin de centraliser la gestion des identités / accès

Concevoir, mettre en place et planifier des solutions d'automatisation (ex : scripts, applications) sur des tâches préalablement identifiées à l'aide d'outils adaptés afin de lancer et d'exécuter de manière automatisée les opérations

Mettre en place un système d'authentification au SI et à ses services afin de permettre un accès sécurisé, conforme et différencié au système d'information (et à ses services)

Mettre en place (installer / configurer / tester / sécuriser) un outil de gestion des actifs et des configurations automatisé, partagé selon les droits définis et accessible, afin de mettre à jour [bénéficier en temps réel des informations sur] les composants du système d'information, préalablement inventoriés, et leurs relations

Définir (choix des méthodes, outils, techniques), installer, configurer et tester une stratégie opérationnelle de sauvegarde en cohérence avec les données (nature / type / criticité) et les contraintes de l'organisation afin d'enregistrer / de dupliquer / de répliquer et d'archiver les données dans un ou plusieurs lieux de stockage selon les critères définis au sein du plan de sauvegarde (classification des données, fréquence souhaitée, etc)

Automatiser les tâches (les opérations) de sauvegarde à l'aide des outils (de planification / d'exécution) et des langages de programmation adaptés (ex : PowerShell, Python, Bash)

Sécuriser, à l'aide des configurations adaptées au plan de sauvegarde et préconisées (ANSSI, fournisseurs, etc), les sauvegardes lors des enregistrements / duplications / répliquions / archivage, afin de réduire les risques d'altération ou de disparition des données

Documenter le système de sauvegarde et établir / formaliser une procédure de restauration des données afin de fournir la démarche à appliquer en cas d'incident

Prioriser et affecter les tickets selon le type / le niveau de support, à l'aide d'un outil de gestion (ex : outil de ticketing / d'assistance) adapté, afin d'organiser les interventions

Effectuer des interventions de support niveaux 2 et/ou 3 afin de rétablir le service fourni au niveau attendu Les enregistrer (demande, réponse apportée, le cas échéant, documentation fournie) afin d'assurer la traçabilité et de clôturer les tickets

Intégrer un outil de supervision, le paramétrer selon le niveau de service attendu (observation des indicateurs de performance / sécurité / disponibilité et seuils) et le tester afin de monitorer les infrastructures informatiques (enregistrer l'activité) et d'émettre une alerte en cas de dysfonctionnements (franchissement du seuil d'alerte)

Établir une procédure afin de présenter le système de supervision auprès de l'équipe en charge de la maintenance du système d'information et les actions à entreprendre en cas de dysfonctionnement / d'alerte (points de contrôles, indicateurs, actions à entreprendre en cas de dysfonctionnement)

Exploiter les remontées (logs / journaux) des activités enregistrées via l'outil de supervision afin d'analyser la performance et la disponibilité des infrastructures informatiques selon les différentes utilisations (spécifiques ou non) au regard des indicateurs définis (ex : taux de disponibilité, charges de calcul, temps de réponse, etc)

Structurer et outiller les différentes étapes d'une intervention portant sur l'évaluation de la sécurité informatique (collecte d'informations, inventaire des actifs, recherche de vulnérabilité, exploitation, élévation des privilèges, propagation, nettoyage) en cohérence avec un périmètre cible

Mettre en œuvre une évaluation de la sécurité informatique sur un périmètre cible, selon la méthodologie préalablement définie et à l'aide des outils adaptés (outils d'énumération / scanner, test d'intrusion, etc) afin d'identifier et de caractériser les vulnérabilités et les failles de sécurité selon leur niveau de criticité

Documenter les vulnérabilités et les failles de sécurité afin de les partager au commanditaire (client interne / externe) Le cas échéant, rédiger des supports à destination d'un public plus élargi (non technique) afin de rendre accessibles les conclusions de l'évaluation

Proposer des mesures ou bien des règles, en cohérence avec les vulnérabilités / failles observées, afin de renforcer la sécurité du SI (mieux protéger / mieux surveiller) Les traduire au sein d'un plan d'action

Modalités d'évaluation :

Mises en situation professionnelle réelles ou reconstituées - Cas pratiques - Soutenances orales.

Blocs de compétences

RNCP40356BC01 - Optimiser (faire évoluer) les infrastructures informatiques

Liste de compétences	Modalités d'évaluation
Définir et mettre en place un système de veille automatisée ou non afin de repérer les évolutions en lien avec son activité (Information Technology / technologies de l'information) Analyser les informations collectées afin d'identifier les opportunités (ex : nouvelles technologies, nouveaux services cloud) et les éventuelles menaces (ex : cybermenaces, mise en conformité nécessaire) Le cas échéant, les partager avec ses pairs (communauté / réseau) ou bien des collaborateurs au sein d'une organisation Analyser, le cas échéant préciser / affiner, et formaliser les besoins informatiques, afin d'identifier les objectifs (résultats attendus) et les éventuelles contraintes techniques, matérielles, budgétaires et réglementaires Identifier une solution en termes d'infrastructure informatique, adaptée et conforme aux besoins / contraintes, à l'aide d'une recherche ponctuelle ciblée ou bien à partir de la veille, et la représenter visuellement, à l'aide d'un outil de modélisation adapté, afin d'en illustrer son implémentation, ses actions et ses éventuels impacts / risques Estimer les coûts associés (humains et matériels) à la solution technique afin de déterminer le budget nécessaire à sa mise en production et à son exploitation Présenter la solution technique, expliquer / argumenter ses choix techniques / financiers auprès des décideurs dans un objectif de validation Organiser (définir / planifier / attribuer) les tâches nécessaires à la conception et à la mise en production de la solution dans le système d'information en cohérence avec les contraintes de l'organisation (notamment un minimum d'impact sur la continuité du service)	Projets (mises en situation professionnelle réelles ou reconstituées, cas pratiques) - Soutenances orales

RNCP40356BC02 - Concevoir et déployer les infrastructures informatiques

Liste de compétences	Modalités d'évaluation
Définir / structurer / modéliser l'architecture technique de l'infrastructure cible, à l'aide d'un logiciel adapté, selon l'agencement des briques fonctionnelles (utilisateurs / données / traitements souhaités) et les critères fournis (performance, sécurité, évolutivité, etc), afin de définir l'organisation et les caractéristiques des équipements / composants et leurs interactions Identifier les configurations à appliquer sur les équipements / composants de l'infrastructure cible, à partir des ressources adaptées (ex : documentation fournisseur) et selon le modèle d'architecture défini afin d'en disposer selon l'usage voulu Créer un prototype ou bien une version pilote (une maquette test) de l'infrastructure système / réseau, à l'aide d'un outil de simulation adapté, afin de visualiser et de tester les équipements / composants, leurs interactions et les fonctionnalités associées Valider ou non la mise en production selon les résultats Identifier les règles de durcissement (suppression des services inutiles, forcer la robustesse des mots de passe, etc), à partir des guides externes (ANSSI, fournisseurs, etc), les adapter si besoin aux contraintes de l'organisation afin de sécuriser les infrastructures Installer et effectuer les réglages (configurations / sécurisation) sur les équipements / composants réseaux / systèmes, quel que soit le type d'infrastructure et le mode de déploiement, dans le respect des règles de l'art et selon les caractéristiques techniques et fonctionnelles définies Élaborer et mettre en œuvre une procédure de test afin de valider la conformité et la fonctionnalité de l'infrastructure déployée Rédiger l'ensemble des procédures nécessaires à la mise en production / au déploiement de la solution Former les utilisateurs ou bien communiquer les bonnes pratiques liées à l'utilisation d'un nouveau service afin d'accompagner le changement	Projets (mises en situation professionnelle réelles ou reconstituées, cas pratiques) - Soutenances orales

RNCP40356BC03 - Administrer (exploiter / maintenir) les infrastructures informatiques

Liste de compétences	Modalités d'évaluation
Organiser / mettre à jour un annuaire des rôles / des autorisations associées à l'aide d'un outil adapté selon les droits définis, dans le respect de la politique de sécurité de l'organisation et de la réglementation en vigueur (sur les données) afin de centraliser la gestion des identités / accès Concevoir, mettre en place et planifier des solutions d'automatisation (ex : scripts, applications) sur des tâches préalablement identifiées à l'aide d'outils adaptés afin de lancer et d'exécuter de manière automatisée les opérations Mettre en place un système d'authentification au SI et à ses services afin de permettre un accès sécurisé, conforme et différencié au système d'information (et à ses services) Mettre en place (installer / configurer / tester / sécuriser) un outil de gestion des actifs et des configurations automatisé, partagé selon les droits définis et accessible, afin de mettre à jour [bénéficier en temps réel des informations sur] les composants du système d'information, préalablement inventoriés, et leurs relations Définir (choix des méthodes, outils, techniques), installer, configurer et tester une stratégie opérationnelle de sauvegarde en cohérence avec les données (nature / type / criticité) et les contraintes de l'organisation afin d'enregistrer / de dupliquer / de répliquer et d'archiver les données dans un ou plusieurs lieux de stockage selon les critères définis au sein du plan de sauvegarde (classification des données, fréquence souhaitée, etc) Automatiser les tâches (les opérations) de sauvegarde à l'aide des outils (de planification / d'exécution) et des langages de programmation adaptés (ex : PowerShell, Python, Bash) Sécuriser, à l'aide des configurations adaptées au plan de sauvegarde et préconisées (ANSSI, fournisseurs, etc), les sauvegardes lors des enregistrements / duplications / répliquions / archivage, afin de réduire les risques d'altération ou de disparition des données Documenter le système de sauvegarde et établir / formaliser une procédure de restauration des données afin de fournir la démarche à appliquer en cas d'incident Prioriser et affecter les tickets selon le type / le niveau de support, à l'aide d'un outil de gestion (ex : outil de ticketing / d'assistance) adapté, afin d'organiser les interventions	Projets (mises en situation professionnelle réelles ou reconstituées, cas pratiques) - Soutenances orales

Liste de compétences	Modalités d'évaluation
Effectuer des interventions de support niveaux 2 et/ou 3 afin de rétablir le service fourni au niveau attendu Les enregistrer (demande, réponse apportée, le cas échéant, documentation fournie) afin d'assurer la traçabilité et de clôturer les tickets	

RNCP40356BC04 - Superviser et surveiller les infrastructures informatiques

Liste de compétences	Modalités d'évaluation
Intégrer un outil de supervision, le paramétrer selon le niveau de service attendu (observation des indicateurs de performance / sécurité / disponibilité et seuils) et le tester afin de monitorer les infrastructures informatiques (enregistrer l'activité) et d'émettre une alerte en cas de dysfonctionnements (franchissement du seuil d'alerte) Établir une procédure afin de présenter le système de supervision auprès de l'équipe en charge de la maintenance du système d'information et les actions à entreprendre en cas de dysfonctionnement / d'alerte (points de contrôles, indicateurs, actions à entreprendre en cas de dysfonctionnement) Exploiter les remontées (logs / journaux) des activités enregistrées via l'outil de supervision afin d'analyser la performance et la disponibilité des infrastructures informatiques selon les différentes utilisations (spécifiques ou non) au regard des indicateurs définis (ex : taux de disponibilité, charges de calcul, temps de réponse, etc) Structurer et outiller les différentes étapes d'une intervention portant sur l'évaluation de la sécurité informatique (collecte d'informations, inventaire des actifs, recherche de vulnérabilité, exploitation, élévation des privilèges, propagation, nettoyage) en cohérence avec un périmètre cible Mettre en œuvre une évaluation de la sécurité informatique sur un périmètre cible, selon la méthodologie préalablement définie et à l'aide des outils adaptés (outils d'énumération / scanner, test d'intrusion, etc) afin d'identifier et de caractériser les vulnérabilités et les failles de sécurité selon leur niveau de criticité Documenter les vulnérabilités et les failles de sécurité afin de les partager au commanditaire (client interne / externe) Le cas échéant, rédiger des supports à destination d'un public plus élargi (non technique) afin de rendre accessibles les conclusions de l'évaluation Proposer des mesures ou bien des règles, en cohérence avec les vulnérabilités / failles observées, afin de renforcer la sécurité du SI (mieux protéger / mieux surveiller) Les traduire au sein d'un plan d'action	Projets (mises en situation professionnelle réelles ou reconstituées, cas pratiques) - Soutenances orales

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

Le référentiel de certification est organisé autour de quatre blocs de compétences, qui peuvent être évalués et validés de manière indépendante. Pour bénéficier de la certification professionnelle complète, le candidat doit valider les quatre blocs de compétences.

Secteur d'activité et type d'emploi

Secteurs d'activités :

Tous secteurs d'activité.

Type d'emplois accessibles :

Administrateur informatique

Administrateur systèmes et réseaux

Administrateur sécurité informatique

Administrateur de serveurs

Administrateur infrastructures

Administrateur Linux / Windows

Code(s) ROME :

M1801 - Administration de systèmes d'information

Références juridiques des réglementations d'activité :

La profession n'est pas réglementée. L'administrateur systèmes, réseaux et cybersécurité exerce toutefois ses activités dans le respect des bonnes pratiques de la profession (sécurité, confidentialité, qualité, numérique responsable...) ainsi que de la législation en vigueur (RGPD, Loi Informatique et Libertés, normes ISO 27000, directives de l'ANSSI...).

Voie d'accès**Le cas échéant, prérequis à l'entrée en formation :**

Être titulaire d'une certification professionnelle de niveau 5 (ou équivalent) en informatique et systèmes d'information ;

OU être titulaire du baccalauréat ou d'une certification de niveau 4 (ou équivalent) et justifier d'une expérience professionnelle d'au moins deux ans en informatique et systèmes d'information.

Tout autre profil relève d'une procédure dérogatoire.

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

Pour bénéficier de la certification professionnelle complète, le candidat doit valider les quatre blocs de compétences.

Pré-requis distincts 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 délivrance de la certification est composé du responsable pédagogique de la filière et deux professionnels du métier visé extérieurs à l'organisme.	-
En contrat d'apprentissage	X		Le jury de délivrance de la certification est composé du responsable pédagogique de la filière et deux professionnels du métier visé extérieurs à l'organisme.	-
Après un parcours de formation continue	X		Le jury de délivrance de la certification est composé du responsable pédagogique de la filière et deux professionnels du métier visé extérieurs à l'organisme.	-
En contrat de professionnalisation	X		Le jury de délivrance de la certification est composé du responsable pédagogique de la filière et deux professionnels du métier visé extérieurs à l'organisme.	-

Voie d'accès à la certification	Oui	Non	Composition des jurys	Date de dernière modification
Par candidature individuelle		X	-	-
Par expérience	X		Le jury de délivrance de la certification est composé du responsable pédagogique de la filière et deux professionnels du métier visé extérieurs à l'organisme.	-

	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

Anciennes versions de la certification professionnelle reconnues en correspondance totale :

Code et intitulé de la certification professionnelle reconnue en correspondance
<u>RNCP36370 - Administrateur systèmes, réseaux et sécurité</u>

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
RNCP40356BC01 - Optimiser (faire évoluer) les infrastructures informatiques	<u>RNCP36370 - Administrateur systèmes, réseaux et sécurité</u>	RNCP36370BC01 - Modéliser, concevoir et documenter un SI sécurisé
RNCP40356BC02 - Concevoir et déployer les infrastructures informatiques	<u>RNCP36370 - Administrateur systèmes, réseaux et sécurité</u>	RNCP36370BC02 - Mettre en production et déployer un SI sécurisé
RNCP40356BC03 - Administrer (exploiter / maintenir) les infrastructures informatiques	<u>RNCP36370 - Administrateur systèmes, réseaux et sécurité</u>	RNCP36370BC03 - Administrer et maintenir un SI au quotidien

Bloc(s) de compétences concernés	Code et intitulé de la certification professionnelle reconnue en correspondance partielle	Bloc(s) de compétences en correspondance partielle
RNCP40356BC04 - Superviser et surveiller les infrastructures informatiques	<u>RNCP36370 - Administrateur systèmes, réseaux et sécurité</u>	RNCP36370BC04 - Superviser, contrôler, optimiser un SI en continu

Base légale

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

Date du JO/BO	Référence au JO/BO
26/04/2022	Date de décision : 26/04/2022 - Durée de l'enregistrement en années : 3 ans - Date d'échéance de l'enregistrement : 26/04/2025

Date de décision	28-03-2025
Durée de l'enregistrement en années	5
Date d'échéance de l'enregistrement	28-03-2030
Date de dernière délivrance possible de la certification	27-03-2034

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 %)
2023	101	8	83	56	-
2022	127	0	89	73	76
2021	34	0	91	68	76

Lien internet vers le descriptif de la certification :

<https://openclassrooms.com/fr/paths/734-administrateur-systemes-reseaux-et-securite>

Liste des organismes préparant à la certification :**Liste des organismes préparant à la certification****Historique des changements de certificateurs :**

Nom légal du certificateur	Siret du certificateur	Action	Date de la modification
OPENCLASSROOMS	49386136300080	Est retiré	19-02-2026
OPENCLASSROOMS	49386136300098	Est ajouté	19-02-2026

Certification(s) antérieure(s) :

Code de la fiche	Intitulé de la certification remplacée
<u>RNCP36370</u>	Administrateur systèmes, réseaux et sécurité

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