

Concepteur intégrateur d'infrastructures informatiques (systèmes et réseaux, applicatives, ou de sécurité)

RNCP38461 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Code(s) NSF	326
Formacode(s)	24231, 31009
Code(s) ROME	M1801, M1805
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	21/12/2023
Date d'échéance	21/12/2028

Certificateur(s)

CONSERVATOIRE NATIONAL DES ARTS ET METIERS · SIRET : 19753471200017

Partenaires habilités

24 organismes habilités, d'après la liste publiée par France compétences : 24 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
AFPI BRETAGNE	30824995200059	Former et organiser l'évaluation
ASSOCIATION DE GESTION DU CNAM DE MARTINIQUE	39064039900015	Former et organiser l'évaluation
ASSOCIATION DE GESTION DU CNAM EN REGION OCCITANIE	49189213900016	Former et organiser l'évaluation
ASSOCIATION DE GESTION DU CONSERVATOIRE DES ARTS ET METIERS	34896746400028	Former et organiser l'évaluation
ASSOCIATION DE GESTION DU CONSERVATOIRE NATIONAL DES ARTS ET METIERS DE LA REUNION	44338132200025	Former et organiser l'évaluation
ASSOCIATION DE GESTION DU CONSERVATOIRE NATIONAL DES ARTS ET METIERS EN GUADELOUPE	39174243400015	Former et organiser l'évaluation
ASSOCIATION DE GESTION DU CONSERVATOIRE NATION DES ARTS ET METIERS AUVERGNE-RHONE-ALPES	44320628900045	Former et organiser l'évaluation
ASSOCIATION MILLAVOISE POUR L'INSERTION ET L'ORIENTATION	34748867800025	Former et organiser l'évaluation
CFAI DIAFOR	39048242000028	Former et organiser l'évaluation
CNAM BOURGOGNE FRANCHE-COMTE	34022316300023	Former et organiser l'évaluation

Liste complète des 24 partenaires habilités : <https://data.aktaconseil.fr/certifications/rncp38461-concepteur-integrateur-d-infrastructures-informatiques-systemes-et-reseaux-applicatives-ou-de-securite/partenaires>

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le poids économique du secteur de l'informatique et du numérique sur le marché ne pourrait se concrétiser que par l'intégration des professionnels disposant des compétences nécessaires pour permettre aux grandes et moyennes entreprises du secteur de rester concurrentielles et de s'adapter à ce marché économique extrêmement vaste. L'utilisation des outils informatiques, les communications terrestres ou satellitaires et les systèmes d'information prennent une place de plus en plus importante dans les entreprises. La transformation digitale accélérée par la crise sanitaire du COVID 19, explique le besoin grandissant en recrutement dans les métiers de l'informatique.

L'évolution du secteur et l'arrivée des nouvelles technologies obligent l'évolution d'infrastructures applicatives, réseaux et systèmes ou de sécurité. Les métiers de ce domaine ont pour objet la conception, le développement, l'exploitation et la maintenance des systèmes informatiques (France Stratégie, 2017). De la conception, le développement, le test vers une intégration et une interopérabilité des services numériques, les professionnels, y compris les concepteurs intégrateurs d'infrastructures informatiques, sont obligés de rester et/ou mettre à jour leurs compétences.

Depuis son premier enregistrement en 2006 l'évolution du marché de l'emploi, de l'attente et des besoins des entreprises en termes de compétences métiers ont permis de faire évoluer le référentiel de la certification professionnelle afin de l'adapter pour répondre à ces nouvelles exigences. La certification maintient son articulation autour d'un tronc commun, qui constitue le socle de compétences incontournables au métier, et de trois options réunissant des compétences spécifiques : « Infrastructures applicatives », « Infrastructures Réseaux et systèmes » et « Cybersécurité ».

ACTIVITÉS VISÉES

Pour concevoir un composant informatique utilisable dans l'infrastructure applicative, système, technique ou de la sécurité d'un Système d'Information d'une entreprise.

Recueil des besoins, capture et analyse des exigences fonctionnelles et non fonctionnelles du composant informatique à concevoir (solution informatique, logiciel) et contribution à la rédaction du cahier des charges du composant informatique à concevoir (solution informatique, logiciel).

Elaboration des spécifications générales du composant informatique à concevoir.

Elaboration des spécifications techniques détaillées du composant informatique à développer.

Pour développer, tester et intégrer un composant informatique dans l'infrastructure applicative, système, technique ou de la sécurité d'un Système d'Information d'une entreprise.

Développement d'un composant informatique dans l'infrastructure applicative, système, technique ou de la sécurité d'un Système d'Information d'une entreprise

Test du composant informatique dans l'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise.

Intégration du composant informatique développé et testé dans l'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise.

Pour analyser et qualifier l'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise

Analyse de l'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise au regard des normes et référentiels en vigueur.

Exécution ou conduite des protocoles de qualification de l'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise.

Pour maintenir en condition opérationnelle une infrastructure applicative.

Gestion des incidents et supervision d'une infrastructure applicative.

Evolution de l'infrastructure applicative.

Pour maintenir en condition opérationnelle une infrastructure réseaux et système.

Gestion des incidents et supervision d'une infrastructure réseaux et système.

Evolution de l'infrastructure réseaux et système compte tenu des évolutions fonctionnelles et non fonctionnelles.

Pour maintenir en condition opérationnelle une infrastructure de sécurité

Gestion des incidents et supervision d'une infrastructure de sécurité.

Evolution de l'infrastructure de sécurité compte tenu des évolutions fonctionnelles et non fonctionnelles.

Pour analyser, organiser et piloter des projets informatiques de développement d'une infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise.

Analyse de projets informatiques de développement d'une infrastructure applicative, système, technique ou de

sécurité d'un Système d'Information d'une entreprise.

Organisation et pilotage des projets informatiques de développement d'une infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise.

COMPÉTENCES ATTESTÉES

BLOC 1?: Concevoir un composant informatique utilisable dans l'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise.

Analyser le/les sous-système(s) du système d'information concerné par le composant informatique à concevoir afin de comprendre son intérêt, rôle, interactions avec le/les sous –système.

Participer à l'organisation et l'animation des réunions de travail en anglais ou en français afin d'apporter son concours au recueil des exigences/besoins des utilisateurs (exigences métiers).

Recueillir, en s'appuyant sur les méthodes et outils d'analyse (approche par les buts, ..) des besoins, les exigences de toutes les parties prenantes (exigences fonctionnelles et non-fonctionnelles) associées au composant informatique à concevoir.

Vérifier la conformité des exigences/besoins identifiés avec les normes (ISO27000x,...) et réglementations (RGPD, réglementation liée à l'accessibilité ..) en vigueur dans le contexte national et international de l'entreprise.

Traduire les exigences fonctionnelles et non fonctionnelles du métier dans un langage formel ou semi-formel (UML,...) en utilisant des méthodes de spécification des besoins afin de s'assurer de leur compréhension, leur clarté, leur exhaustivité, et de leur cohérence.

Participer à la rédaction, en anglais ou en français, du cahier des charges du composant informatique à concevoir en s'appuyant sur les modèles standards (normes ISO29148,...) en vigueur dans l'entreprise.

Analyser le cahier des charges, en s'appuyant sur des méthodes d'analyse et de conception de composants informatiques (UML,...) afin d'identifier les solutions techniques (type de base de données, moteur de recherche, méthodes d'authentification, modèle...) répondant aux exigences du métier.

Evaluer la faisabilité technique et économique (POC, MVP, ..) des solutions techniques répondant aux exigences afin d'identifier et proposer à ses responsables le cas échéant, les solutions techniques optimales compte tenu des besoins/identifiés.

Sélectionner ou proposer la solution technique optimale au regard de l'équilibre entre coût et qualité, afin de la consigner dans un document de spécification technique servant d'appui à la mise en œuvre du composant informatique.

Concevoir les modèles et schémas associés à la conception du composant informatique et de son environnement informatique en utilisant les modèles formels ou semi-formels (modèle d'authentification, modèle de données, modèle de menaces à l'aide des TTP par exemple, un diagramme de séquence, un diagramme d'activités,...) afin de préparer le développement et l'évolution du composant informatique.

Rédiger les spécifications techniques détaillées servant d'appui à la mise en œuvre du composant informatique à développer sur la base des spécifications générales et des référentiels techniques existants et dans le respect du cahier de charges

Soumettre la spécification technique détaillée produite à la validation des parties prenantes impliquées dans le projet (décideurs, utilisateurs,) en veillant à ce qu'elle soit adaptée au niveau de compréhension de l'ensemble des acteurs.

BLOC 2 : Développer, tester et intégrer un composant informatique dans l'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise

Préparer la mise en œuvre d'une solution technique détaillée (réunir les logiciels, choisir les outils et les paramétrer, rédiger les procédures ...) afin de réaliser une solution technique.

Mettre en œuvre une solution technique associée à un composant informatique du SI et documentée dans une spécification technique, en agissant dans le respect des normes de développement (ex. qualité) et du cahier des charges et en suivant une méthodologie de construction (exemple démarche Devops) afin de produire le composant.

Elaborer les tests et rédiger les cahiers de tests en transcrivant les exigences fonctionnelles et non fonctionnelles sous forme de cas de tests et en s'aidant de méthodes de tests appropriées (test d'intrusion, test de vulnérabilité, les tests unitaires, tests d'intégration ,...) afin de valider

la solution technique produite.

Exécuter, ou faire exécuter par son équipe, les différents tests unitaires en analysant le comportement d'un composant ou des éléments constituant le composant à l'aide d'outils (WireShark, Kali linux, OWASP, ...) afin d'identifier d'éventuelles anomalies et de définir les réajustements à faire pour chacune des anomalies détectées.

Appliquer les réajustements proposés par son équipe ou par un partenaire dans le respect des exigences afin de produire ou faire produire une nouvelle version de tout ou partie du composant.

Intégrer le composant développé dans son environnement d'exploitation, tout en respectant les procédures établies et le cahier de charges afin de le rendre opérationnel au sein du SI.

Vérifier l'exploitabilité du composant développé et intégré sous un environnement de pré-production afin de le rendre opérationnel au sein du Système d'information.

BLOC 3 : Analyser et qualifier l'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise

Conduire une étude de l'infrastructure, en s'appuyant sur des méthodes d'analyse de risque et sur les exigences normatives et réglementaires en vigueur (EBIOS, ISO27X, COBIT, RFC,...) afin d'identifier les composants critiques de l'infrastructure nécessitant des actions de qualification.

Consolider les processus mis en place garantissant la pérennité de l'état qualifié d'une l'infrastructure pour donner suite à l'évolution des exigences normatives et réglementaires en vigueur tel que : la politique de sécurité PSSI.

Définir, les protocoles de validation informatique et de qualification en s'appuyant aussi sur les méthodes/guides/normes reconnus (ISO 19011, OWASP "Open Web Application Security Project" Testing Guide, etc.) de vérifier et de valider la maintenabilité, la performance, la qualité, la robustesse et l'évolutivité de l'infrastructure.

Rédiger des protocoles de validation informatique et de qualification en intégrant les codes et contraintes spécifiques de l'entreprise afin d'exécuter l'analyse de l'infrastructure.

Exécuter ou faire exécuter par son équipe des protocoles de validation informatique et de qualification en s'appuyant sur des outils d'audits (Checkmarx, NMAP, tests d'intrusions, Metasploit, etc.) afin d'identifier d'éventuelles déviations (problèmes de performance, sécurité, structuration de code, etc.).

Investiguer sur les déviations identifiées (problèmes de performance, sécurité, structuration de code, ...) par rapport aux objectifs fixés, en s'appuyant sur des outils ou approches d'investigation (Metasploit, Kali-linux,...) afin d'établir un diagnostic de l'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise.

Proposer et consigner dans un document des mesures correctives (réviser le code, utiliser des patrons de conception, adapter l'infrastructure réseau ou de sécurité aux nouveaux standards et normes, sécurisation des serveurs, etc..) afin de pallier des déviations constatées et de les exécuter ou les faire exécuter par son équipe.

Exécuter ou faire exécuter par son équipe des mesures correctives en utilisant l'approche PDCA (Plan Do Check Act) afin de pallier des déviations constatées.

BLOC 4 - Option Système d'information : Maintenir en condition opérationnelle une infrastructure applicative

Mettre en place des solutions de recueil des incidents pouvant survenir sur l'infrastructure applicative (Request Tracker, ITop, GLPI, etc...), des tableaux de bord de suivi des incidents et de qualité des infrastructures applicatives de l'entreprise afin de répondre et traiter les incidents de l'infrastructure applicative (lenteur de réponse d'application, dysfonctionnement ou crash de d'application, etc ...).

Analyser les incidents (indisponibilité des ressources, problème de transfert de données, etc..) survenus sur un composant de l'infrastructure applicative en s'appuyant sur des méthodes d'analyse des incidents appropriées (ITIL, etc ..) afin d'y remédier.

Résoudre ou faire résoudre par son équipe tout signalement d'incidents survenus dans l'infrastructure applicative (correction de bug, optimisation d'une base, révision de l'interface utilisateur, ..), en tenant compte de l'analyse effectuée préalablement afin de rétablir et de garantir la continuité du service offert.

Appliquer ou faire appliquer par son équipe les directives de sécurité associées à l'infrastructure applicative (déploiement des mises à jour, chiffrement des données, anonymisation des données sensibles, sauvegarde, gestion des droits d'accès aux applicatifs, ... etc)

afin de garantir la continuité du service offert.

Echanger avec les utilisateurs (entretiens, enquêtes) sur les applicatifs afin de recueillir les améliorations qu'ils souhaitent (ergonomie des interfaces, amélioration du temps de réponse des applicatifs..).

Gérer le portefeuille applicatif (montée des versions, ajout de fonctionnalités, révision du paramétrage d'un progiciel, migration, etc.), en appliquant les améliorations souhaitées par les utilisateurs afin de maintenir leur satisfaction ou en s'appuyant sur les indicateurs et axes d'analyse dans les différents domaines liés à l'exploitation du logiciel.

Assurer une veille technologique sur les composants stratégiques de l'infrastructure applicative (les systèmes de gestion de bases de données, des solutions métier) afin de répondre à des besoins futurs (montée en version des logiciels, ergonomie et accessibilité de l'interface, automatisation des fonctionnalités de l'infrastructure applicative).

Assurer ou coordonner la maintenance corrective des applicatifs afin de garantir la continuité des services offerts par les applicatifs.

Optimiser l'organisation et les performances des composants de l'infrastructure applicative en réalisant des statistiques des performances d'accès (optimisation des requêtes d'accès aux bases de données, etc) afin de

maintenir la qualité de service préconisée.

BLOC 5 - Option Système et réseaux : Maintenir en condition opérationnelle une infrastructure réseaux et système.

Mettre en place des solutions de supervision et des tableaux de bord de suivi des performances et de qualité des infrastructures réseaux et système de l'entreprise (Nagios, SNMP, Observium ...) afin de répondre et traiter incidents réseaux et système (saturation de la bande passante, rupture des flux, perte d'un équipement, etc ...).

Analyser les incidents de réseaux et système (pannes ou dysfonctionnements, etc ..) à partir de traces (journaux d'évènements, graphes d'usage de ressources, historique de consommation, bande passante, performance des systèmes,

..) survenus sur un composant de l'infrastructure informatique en s'appuyant par exemple sur des outils de capture et d'analyse de trames (Wireshark,..) afin d'y remédier.

Réparer ou faire réparer par son équipe tout signalement de pannes ou de dysfonctionnements des équipements de l'infrastructure réseaux et système (routeurs, commutateurs, serveurs, services,), en tenant compte de l'analyse effectuée préalablement afin de rétablir et de garantir la continuité du service offert.

Appliquer ou faire appliquer par son équipe les directives de sécurité associées à l'infrastructure réseaux et système (déploiement des mises à jour, protection des infrastructures, chiffrement des données et des communications, anonymisation des données sensibles, sauvegarde, gestion des droits, etc)

afin de garantir la continuité du service offert.

Analyser les remontées des utilisateurs quant à la qualité des services de l'infrastructure réseau système afin de mettre en place les améliorations qu'ils souhaitent (augmentation débit réseau, augmentation des ressources systèmes tels que : espace disque, CPU ou RAM, meilleure disponibilité des services, etc).

Réaliser une veille sur les matériels et systèmes des composants de l'infrastructure informatique afin de faire évoluer l'infrastructure et l'adapter aux besoins des utilisateurs (amélioration des débits, nouvelles versions des systèmes, évolution des services, etc...).

Prévoir et réaliser ou faire réaliser par son équipe des diagnostics de l'infrastructure réseaux et système (démarche préventive) afin d'éviter toute source de problèmes informatiques qui remettrait en cause qualité de service des composants de l'infrastructure réseaux et système.

Optimiser l'organisation et les performances des composants de l'infrastructure réseaux et système afin de maintenir la qualité de service préconisée.

BLOC 6 - Option Cybersécurité : Maintenir les conditions de sécurité d'un système d'information et de son infrastructure de sécurité.

Mettre en place des solutions de supervision des infrastructures de sécurité de l'entreprise (outils SIEM tel que : splunk, ELK, IDS...) afin de répondre et traiter incidents de sécurité (déni de service, intrusions, ..).

Réaliser une veille sur les vulnérabilités (logicielles et matérielles) des composants de l'infrastructure informatique afin de se conformer à la politique de sécurité (appliquer les mises à jour sur les systèmes informatiques de l'entreprise tel que : PATCH de sécurité, renforcement des authentifications, ETC,...).

Analyser les incidents de sécurité à partir de traces ou de codes informatiques (codes malveillants, journaux d'évènements,) survenus sur un composant de l'infrastructure informatique en s'appuyant par exemple sur des méthodes d'analyse inverse automatisées tel que : le « fuzzing » d'analyse de codes binaires ou manuelles tel que l'analyse statique afin d'y remédier.

Anticiper les incidents de sécurité, au moyen d'outils de la cyber threat intelligence (OpenCTI) et en appréhendant les nouvelles menaces et contremesures afin d'assurer le maintien des conditions opérationnelles de sécurité et de prendre en compte les évolutions liées aux menaces émergentes et systémiques (stuxnet, pegasus, rançongiciels, phishing,).

Assurer ou coordonner la réponse à un incident de sécurité par exemple en situation de crise afin de garantir la continuité ou la reprise des services offerts par le système d'information de l'entreprise.

Optimiser les infrastructures de sécurité en réalisant des campagnes de métrologie et/ou audits (mettre à niveau et faire évoluer les règles de parefeux, mettre à niveau les règles de corrélation des SIEM, ...) afin de maintenir les conditions de sécurité préconisée.

BLOC 7 : Analyser, organiser et piloter des projets informatiques de développement d'une infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise.

Analyser les caractéristiques du projet (objectifs, contraintes, risques, contexte, ...) afin de définir le planning de réalisation du projet (ordonnancement et échéances des actions,

..).

Participer aux choix de progiciels, d'outils et/ou de technologies, en veillant au respect du cahier des charges, en

réalisant une veille technologique et en mobilisant des expertises afin d'assurer la réussite du projet.

Utiliser les méthodes gestion de projet (cycle en V, méthodes AGILE, ...) et outils (JIRA, CONFLUENCE, diagramme de Gantt,

..) en veillant au respect du cahier des charges et au respect des exigences de qualité et de sécurité ainsi qu'au respect des réglementations en vigueur (PCI DSS, RGPD, ...) afin de piloter des projets de développement informatique.

Communiquer régulièrement à l'oral et à l'écrit sur l'état d'avancement du projet et les aléas potentiels (délais, coûts, volume et qualité des fonctionnalités) à sa hiérarchie ou au donneur d'ordres en interne et externe, en anglais ou en français, en fonction de l'interlocuteur (l'équipe de projet et/ou la maîtrise d'ouvrage).

Animer une petite équipe d'un à six informaticiens (fixer des objectifs, répartir l'activité, motiver, évaluer, etc.), en s'appuyant sur des méthodes de gestion d'équipes et des outils collaboratifs (Daily meeting, scrum board,...) afin de répondre à une demande de développement ou de déploiement d'un composant.

Mettre en place et affecter à chaque collaborateur de l'équipe les actions à réaliser dans le cadre du projet en tenant compte des objectifs du projet (qualitatifs et quantitatifs) et des compétences de chacun afin de mener à terme un projet de conception/ développement/évolution d'un composant d'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise.

Assurer le rôle de support technique et d'assistance auprès des équipes informatiques dans le cadre de son périmètre d'expertise (assistance en cas de blocage, élaboration de supports de formation, tutoriels d'intégration et utilisation, FAQ,

..) afin de garantir la qualité technique du projet.

Assurer et adapter la communication interne et externe, en anglais ou en français, en fonction de l'interlocuteur (l'équipe de projet et/ou la maîtrise d'ouvrage).

Appliquer, en lien avec la cellule handicap / service RH de l'entreprise, les procédures et aménagements adaptées à la situation des personnes en situation de handicap intégrées dans le projet (postes de travail, moyens de communication, outils de collaboration et de communication adaptés,...) au regard des éventuels préconisations émises par le médecin du travail afin de structurer la prise en compte du handicap au sein de l'équipe informatique.

Rédiger en français ou en anglais de l'ensemble des livrables du projet (manuels d'utilisation, manuels d'intégration, manuel de déploiement, manuels d'exploitation, etc.) afin d'en assurer l'utilisation optimale par les entités cible de l'entreprise (exploitants, équipe de la mise en production, utilisateurs du service et/ou de l'application,/ du composant informatique,...).

Blocs de compétences

RNCP38461BC01 — Concevoir un composant informatique utilisable dans l'infrastructure applicative, système, technique ou de la sécurité d'un Système d'Information d'une entreprise

LISTE DE COMPÉTENCES

Analyser le/les sous-système(s) du système d'information concerné par le composant informatique à concevoir afin de comprendre son intérêt, rôle, interactions avec le sous –système.

Participer à l'organisation et l'animation des réunions de travail en anglais ou en français afin d'apporter son concours au recueil des exigences/besoins des utilisateurs (exigences métiers).

Recueillir, en s'appuyant sur les méthodes et outils d'analyse (approche par les buts, ..) des besoins, les exigences de toutes les parties prenantes (exigences fonctionnelles et non-fonctionnelles) associées au composant informatique à concevoir.

Vérifier la conformité des exigences/besoins identifiés avec les normes (ISO27000x,...) et réglementations (RGPD, réglementation liée à l'accessibilité ..) en vigueur dans le contexte national et international de l'entreprise.

Traduire les exigences fonctionnelles et non fonctionnelles du métier dans un langage formel ou semi-formel (UML,...) en utilisant des méthodes de spécification des besoins afin de s'assurer de leur compréhension, leur clarté, leur exhaustivité, et de leur cohérence.

Participer à la rédaction, en anglais ou en français, du cahier des charges du composant informatique à concevoir en s'appuyant sur les modèles standards (normes ISO29148,...) en vigueur dans l'entreprise.

MODALITÉS D'ÉVALUATION

Evaluations écrites en groupe (2 à 4 personnes);

Etudes de cas.

RNCP38461BC02 — Développer, tester et intégrer un composant informatique dans l'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise

LISTE DE COMPÉTENCES

Préparer la mise en œuvre d'une solution technique détaillée (réunir les logiciels, choisir les outils et les paramétrer, rédiger les procédures ...) afin de réaliser une solution technique.

Mettre en œuvre une solution technique associée à un composant informatique du SI et documentée dans une spécification technique, en agissant dans le respect des normes de développement (ex. qualité) et du cahier des charges et en suivant une méthodologie de construction afin de produire le composant.

Elaborer les tests et rédiger les cahiers de tests en transcrivant les exigences fonctionnelles et non fonctionnelles sous forme de cas de tests et en s'aidant de méthodes de tests appropriées (test d'intrusion, test de vulnérabilité, les tests unitaires, tests d'intégration, ...) afin de valider

la solution technique produite.

Exécuter, ou faire exécuter par son équipe, les différents tests unitaires

en analysant le comportement d'un composant ou des éléments constituant le composant à l'aide d'outils (WireShark, Kali linux, OWASP, ...) afin d'identifier d'éventuelles anomalies et de définir les réajustements à faire pour chacune des anomalies détectées.

Appliquer les réajustements proposés par son équipe ou par un partenaire dans le respect des exigences afin de produire ou faire produire une nouvelle version de tout ou partie du composant.

Intégrer le composant développé dans son environnement d'exploitation, tout en respectant les procédures établies et le cahier de charges afin de le rendre opérationnel au sein du SI.

Vérifier l'exploitabilité du composant développé et intégré sous un environnement de pré-production afin de le rendre opérationnel au sein du Système d'information.

MODALITÉS D'ÉVALUATION

Epreuves en groupes;

Dans le cadre d'un projet, élaboration des cahiers de test d'un composant informatique du SI et rédaction d'un rapport portant sur le projet réalisé.

RNCP38461BC03 — Analyser et qualifier l'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise

LISTE DE COMPÉTENCES

Conduire une étude de l'infrastructure, en s'appuyant sur des méthodes d'analyse de risque et sur les exigences normatives et réglementaires en vigueur (EBIOS, ISO27X, COBIT, RFC,...) afin d'identifier les composants critiques de l'infrastructure nécessitant des actions de qualification.

Consolider les processus mis en place garantissant la pérennité de l'état qualifié d'une l'infrastructure pour donner suite à l'évolution des exigences normatives et réglementaires en vigueur tel que : la politique de sécurité PSSI.

Définir, les protocoles de validation informatique et de qualification en s'appuyant aussi sur les méthodes/guides/normes reconnus (ISO 19011, OWASP "Open Web Application Security Project" Testing Guide, etc.) de vérifier et de valider la maintenabilité, la performance, la qualité, la robustesse et l'évolutivité de l'infrastructure.

Rédiger des protocoles de validation informatique et de qualification en intégrant les codes et contraintes spécifiques de l'entreprise afin d'exécuter l'analyse de l'infrastructure.

Exécuter ou faire exécuter par son équipe des protocoles de validation informatique et de qualification en s'appuyant sur des outils d'audits (Checkmarx, NMAP, tests d'intrusions, Metasploit, etc.) afin d'identifier d'éventuelles déviations (problèmes de performance, sécurité, structuration de code, etc.).

Investiguer sur les déviations identifiées (problèmes de performance, sécurité, structuration de code, ...) par rapport aux objectifs fixés, en s'appuyant sur des outils ou approches d'investigation (Metasploit, Kali-linux,...) afin d'établir un diagnostic de l'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise.

Proposer et consigner dans un document des mesures correctives (réviser le code, utiliser des patrons de conception, adapter l'infrastructure réseau ou de sécurité aux nouveaux standards et normes, sécurisation des serveurs, etc..) afin de pallier des déviations constatées et de les exécuter ou les faire exécuter par son équipe.

Exécuter ou faire exécuter par son équipe des mesures correctives en utilisant l'approche PDCA (Plan Do Check Act) afin de pallier des déviations constatées

MODALITÉS D'ÉVALUATION

Etude de cas ;

Epreuve individuelle écrite ;
Epreuve individuelle sur poste informatique et sur table.

RNCP38461BC04 — Maintenir en condition opérationnelle une infrastructure applicative (Option)

LISTE DE COMPÉTENCES

Mettre en place des solutions de recueil des incidents pouvant survenir sur l'infrastructure applicative (Request Tracker, ITop, GLPI, etc...), des tableaux de bord de suivi des incidents et de qualité des infrastructures applicatives de l'entreprise afin de répondre et traiter les incidents de l'infrastructure applicative (lenteur de réponse d'application, dysfonctionnement ou crash de d'application, etc ...).

Analyser les incidents (indisponibilité des ressources, problème de transfert de données, etc..) survenus sur un composant de l'infrastructure applicative en s'appuyant sur des méthodes d'analyse des incidents appropriées (ITIL, etc ..) afin d'y remédier.

Résoudre ou faire résoudre par son équipe tout signalement d'incidents survenus dans l'infrastructure applicative (correction de bug, optimisation d'une base, révision de l'interface utilisateur, ..), en tenant compte de l'analyse effectuée préalablement afin de rétablir et de garantir la continuité du service offert.

Appliquer ou faire appliquer par son équipe les directives de sécurité associées à l'infrastructure applicative (déploiement des mises à jour, chiffrement des données, anonymisation des données sensibles, sauvegarde, gestion des droits d'accès aux applicatifs, ... etc) afin de garantir la continuité du service offert.

Echanger avec les utilisateurs (entretiens, enquêtes) sur les applicatifs afin de recueillir les améliorations qu'ils souhaitent (ergonomie des interfaces, amélioration du temps de réponse des applicatifs, ..).

Gérer le portefeuille applicatif (montée des versions, ajout de fonctionnalités, révision du paramétrage d'un progiciel, migration, etc.), en appliquant les améliorations souhaitées par les utilisateurs afin de maintenir leur satisfaction ou en s'appuyant sur les indicateurs et axes d'analyse dans les différents domaines liés à l'exploitation du logiciel.

Assurer une veille technologique sur les composants stratégiques de l'infrastructure applicative (les systèmes de gestion de bases de données, des solutions métier) afin de répondre à des besoins futurs (montée en version des logiciels, ergonomie et accessibilité de l'interface, automatisation des fonctionnalités de l'infrastructure applicative).

Assurer ou coordonner la maintenance corrective des applicatifs afin de garantir la continuité des services offerts par les applicatifs.

Optimiser l'organisation et les performances des composants de l'infrastructure applicative en réalisant des statistiques des performances d'accès (optimisation des requêtes d'accès aux bases de données, etc) afin de maintenir la qualité de service préconisée.

MODALITÉS D'ÉVALUATION

Etudes de cas ;
Epreuve individuelle écrite;
Epreuve individuelle, orale.

RNCP38461BC05 — Maintenir en condition opérationnelle une infrastructure réseaux et système (option Système et réseaux)

LISTE DE COMPÉTENCES

Mettre en place des solutions de supervision et des tableaux de bord de suivi des performances et de qualité des infrastructures réseaux et système de l'entreprise (Nagios, SNMP, Observium ...) afin de répondre et traiter incidents réseaux et système (saturation de la bande passante, rupture des flux, perte d'un équipement, etc ...).

Analyser les incidents de réseaux et système (pannes ou dysfonctionnements, etc ..) à partir de traces (journaux d'évènements, graphes d'usage de ressources, historique de consommation, bande passante, performance des systèmes,

..) survenus sur un composant de l'infrastructure informatique en s'appuyant par exemple sur des outils de capture et d'analyse de trames (Wireshark,..) afin d'y remédier.

Réparer ou faire réparer par son équipe tout signalement de pannes ou de dysfonctionnements des équipements de l'infrastructure réseaux et système (routeurs, commutateurs, serveurs, services, ..), en tenant compte de l'analyse effectuée préalablement afin de rétablir et de garantir la continuité du service offert.

Appliquer ou faire appliquer par son équipe les directives de sécurité associées à l'infrastructure réseaux et système (déploiement des mises à jour, protection des infrastructures, chiffrement des données et des communications, anonymisation des données sensibles, sauvegarde, gestion des droits, ... etc)

afin de garantir la continuité du service offert.

Analyser les remontées des utilisateurs quant à la qualité des services de l'infrastructure réseau système afin de mettre en place les améliorations qu'ils souhaitent (augmentation débit réseau, augmentation des ressources systèmes tels que : espace disque, CPU ou RAM, meilleure disponibilité des services, etc,...).

Réaliser une veille sur les matériels et systèmes des composants de l'infrastructure informatique afin de faire évoluer l'infrastructure et l'adapter aux besoins des utilisateurs (amélioration des débits, nouvelles versions des systèmes, évolution des services, etc...).

Prévoir et réaliser ou faire réaliser par son équipe des diagnostics de l'infrastructure réseaux et système (démarche préventive) afin d'éviter toute source de problèmes informatiques qui remettrait en cause qualité de service des composants de l'infrastructure réseaux et système.

Optimiser l'organisation et les performances des composants de l'infrastructure réseaux et système afin de maintenir la qualité de service préconisée.

MODALITÉS D'ÉVALUATION

Etude de cas pratique ;

Epreuve individuelle orale ;

Epreuve écrite individuelle et/ou en binômes ;

RNCP38461BC06 — Maintenir les conditions de sécurité d'un système d'information et de son infrastructure de sécurité. (option Cybersécurité)

LISTE DE COMPÉTENCES

Mettre en place des solutions de supervision des infrastructures de sécurité de l'entreprise (outils SIEM tel que : splunk, ELK, IDS...) afin de répondre et traiter incidents de sécurité (déni de service, intrusions, ..).

Réaliser une veille sur les vulnérabilités (logicielles et matérielles) des composants de l'infrastructure informatique afin de se conformer à la politique de sécurité (appliquer les mises à jour sur les systèmes informatiques de l'entreprise tel que : PATCH de sécurité, renforcement des authentifications, ETC,...).

Analyser les incidents de sécurité à partir de traces ou de codes informatiques (codes malveillants, journaux d'événements,) survenus sur un composant de l'infrastructure informatique en s'appuyant par exemple sur des méthodes d'analyse inverse automatisées tel que : le « fuzzing » d'analyse de codes binaires ou manuelles tel que l'analyse statique afin d'y remédier.

Anticiper les incidents de sécurité, au moyen d'outils de la cyber threat intelligence (OpenCTI) et en appréhendant les nouvelles menaces et contremesures afin d'assurer le maintien des conditions opérationnelles de sécurité et de prendre en compte les évolutions liées aux menaces émergentes et systémiques (stuxnet, pegasus, rançongiciels, phishing,).

Assurer ou coordonner la réponse à un incident de sécurité par exemple en situation de crise afin de garantir la continuité ou la reprise des services offerts par le système d'information de l'entreprise.

Optimiser les infrastructures de sécurité en réalisant des campagnes de métrologie et/ou audits (mettre à niveau et faire évoluer les règles de parefeux, mettre à niveau les règles de corrélation des SIEM, ...) afin de maintenir les conditions de sécurité préconisée.

MODALITÉS D'ÉVALUATION

Epreuve individuelle ou en groupe réalisée au moyen d'une plateforme de Cyber entraînement.

RNCP38461BC07 — Analyser, organiser et piloter des projets informatiques de développement d'une infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise.

LISTE DE COMPÉTENCES

Analyser les caractéristiques du projet (objectifs, contraintes, risques, contexte, ...) afin de définir le planning de réalisation du projet (ordonnancement et échéances des actions, ..).

Participer aux choix de progiciels, d'outils et/ou de technologies, en veillant au respect du cahier des charges, en réalisant une veille technologique et en mobilisant des expertises afin d'assurer la réussite du projet.

Utiliser les méthodes gestion de projet (cycle en V, méthodes AGILE, ...) et outils (JIRA, CONFLUENCE, diagramme de Gantt,

..) en veillant au respect du cahier des charges et au respect des exigences de qualité et de sécurité ainsi qu'au respect des réglementations en vigueur (PCI DSS, RGPD, ...) afin de piloter des projets de développement informatique.

Communiquer régulièrement à l'oral et à l'écrit sur l'état d'avancement du projet et les aléas potentiels (délais, coûts, volume et qualité des fonctionnalités) à sa hiérarchie ou au donneur d'ordres en interne et externe, en anglais ou en français, en fonction de l'interlocuteur (l'équipe de projet et/ou la maîtrise d'ouvrage).

Animer une petite équipe d'un à six informaticiens (fixer des objectifs, répartir l'activité, motiver, évaluer, etc.), en s'appuyant sur des méthodes de gestion d'équipes et des outils collaboratifs (Daily meeting, scrum board,...) afin de répondre à une demande de développement ou de déploiement d'un composant.

Mettre en place et affecter à chaque collaborateur de l'équipe les actions à réaliser dans le cadre du projet en tenant compte des objectifs du projet (qualitatifs et quantitatifs) et des compétences de chacun afin de mener à terme un projet de conception/ développement/évolution d'un composant d'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise.

Assurer le rôle de support technique et d'assistance auprès des équipes informatiques dans le cadre de son périmètre d'expertise (assistance en cas de blocage, élaboration de supports de formation, tutoriels d'intégration et utilisation, FAQ,

..) afin de garantir la qualité technique du projet.

Assurer et adapter la communication interne et externe, en anglais ou en français, en fonction de l'interlocuteur (l'équipe de projet et/ou la maîtrise d'ouvrage).

Appliquer, en lien avec la cellule handicap / service RH de l'entreprise, les procédures et aménagements adaptées à la situation des personnes en situation de handicap intégrées dans le projet (postes de travail, moyens de communication, outils de collaboration et de communication adaptés,...) au regard des éventuelles préconisations émises par le médecin du travail afin de structurer la prise en compte du handicap au sein de l'équipe informatique.

Rédiger en français ou en anglais de l'ensemble des livrables du projet (manuels d'utilisation, manuels d'intégration, manuel de déploiement, manuels d'exploitation, etc.) afin d'en assurer l'utilisation optimale

par les entités cible de l'entreprise (exploitants, équipe de la mise en production, utilisateurs du service et/ou de l'application,/ du composant informatique,...).

MODALITÉS D'ÉVALUATION

Epreuve sur un projet tutoré réalisé en petits groupe (de 2 à 5 personnes) ;

Epreuve écrite ;

Présentation orale.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le concepteur intégrateur d'infrastructures informatiques exerce son métier, la plupart du temps, dans des entreprises de service numérique (ESN) ou directement dans les services informatiques d'une entreprise lorsque celle-ci en tire suffisamment de revenus pour en absorber le coût. Toutes les entreprises sont potentiellement recruteuses, les secteurs des entreprises utilisatrices d'informatique sont divers (banque, constructeur automobile, administration, etc.).

TYPE D'EMPLOIS ACCESSIBLES

L'appellation-métier peut varier selon la taille et la nature des activités de l'entreprise au sein duquel le concepteur intégrateur d'infrastructures informatiques exerce le métier. Elle peut recouvrir les termes suivants :

- Concepteur d'application informatique ou concepteur-développeur,
- Analyste (analyste fonctionnel, analyste d'exploitation, analyste système, analyste sécurité),
- Chef de projet informatique,
- Architecte (bases de données, systèmes d'information, réseaux informatiques, système informatique),
- Expert (réseaux, système d'exploitation, système et réseaux, sécurité),
- Administrateur (bases de données, réseau informatique, système, sécurité, d'applications, etc.),
- Responsable informatique,
- Responsable infrastructure informatique
- Responsable d'application,
- Cadre informatique,
- Informaticien.

RÉGLEMENTATIONS D'ACTIVITÉ

Le métier n'est pas réglementé en tant que tel,

mais plusieurs de ses activités s'exercent sous contraintes réglementaires et normatives. La prise en compte de ces contraintes réglementaires et normatives, y compris de sécurité, est répartie et évaluée sur chacun des 4 blocs de tronc commun. Un bloc de spécialisation est dédié au maintien en condition opérationnelle de l'infrastructure de sécurité (option Cybersécurité).

Marché du travail

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

Tension de recrutement (DARES 2024)	Élevée (4/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 690 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (41 % des actifs en emploi)
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique · tension 4/5 (Élevée) M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom · tension 5/5 (Très 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)	37 007
Jugés difficiles à recruter	51 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom 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
Niveau 5 en informatique ou scientifique ou technique non informatique, et Valeurs d'Accueil et de Reconversion (Unités d'Enseignement visant l'acquisition des compétences scientifiques de base/mise à niveau).

COMPOSITION DU JURY — FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION, VAE
Pour 50%
des enseignants du Cnam (soit un représentant de l'Administratrice générale du Cnam et un enseignant-chercheur du Cnam, soit le responsable pédagogique de la certification professionnelle ou son représentant)
Pour 50% des professionnels qualifiés du métier concerné (2 membres extérieurs du Cnam).

ACCESSIBLE EN OUTRE-MER
Nouvelle-Calédonie

Financement en alternance (NPEC)

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

Prise en charge usuelle	7 431 €
Selon la branche	6 500 € – 7 640 €
Prise en charge	Branches concernées
7 431 €	Valeur par défaut · 189 branches
7 640 €	CPNE Banque, CPNE chimie, CPNE de la branche de l'hospitalisation privée à statut commercial et du thermalisme, CPNE des Métiers de la Transformation des Grains, CPNE des industries de santé (CPNEIS)
7 319 €	CPNE Entreprises des activités du déchet et de la propreté urbaine, CPNE des Télécoms, CPNEF de la Branche des organismes de formation, CPNEFP ICGV entreprises de la viande, CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
7 000 €	CPNE Branche Caoutchouc, CPNEFP de la métallurgie
7 604 €	CPNEFP du Négoce de l'ameublement
7 500 €	CPNEFP des commerces de gros
7 440 €	CPNE de l'ingénierie, des services informatiques et du conseil
7 421 €	CPNEFP dans les établissements d'enseignement privés sous contrat
7 300 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
6 500 €	CPNE du Commerce de détail et de gros à prédominance alimentaire

Base légale

Date de décision	21/12/2023
Durée de l'enregistrement	5 ans
Date d'échéance de l'enregistrement	21/12/2028
Date de dernière délivrance possible	21/12/2032

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2021	53	5	81 %	—
2020	45	3	75 %	74 %
2019	67	8	83 %	80 %
2018	68	4	93 %	83 %

Liens avec d'autres certifications

ANCIENNES VERSIONS
RNCP15253

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/38461/>

Où se former

Formations référencées	47
Organismes	11
Régions couvertes	6
Prix indicatif	1 020 € – 14 700 €
Durée	135 – 150 h

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

Se former en apprentissage

Formations en apprentissage	1
Organismes gestionnaires (CFA)	1
Organismes formateurs	1
Régions couvertes	1
Départements couverts	1
Organismes certifiés Qualiopi	1
Sessions	de 09/2025 à 08/2028

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

Entrées et sorties de formation

Entrées en formation	15
Parcours menés à terme	4
Taux d'achèvement	27 %
Période	10/2024 – 09/2026

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

Demande CPF — formations engagées

Dossiers CPF engagés	29
Montant total engagé	62 322 €
Coût moyen par dossier	2 149 €
Durée moyenne	120 h
Période	09/2024 – 09/2026
France compétences	93 %
OPCO	4 %

Reste à charge titulaire

3 %

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