1. Intitulé du certificat (Dans la langue d'origine)

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

2. Traduction de l'intitulé du certificat (Le cas échéant. Cette traduction est dépourvue de toute valeur légale)

3. Eléments de compétences acquis

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, règlementation 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 constituants 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.

Le Supplément au certificat complète l'information figurant sur le certificat/titre/diplôme. Ce document n'a aucune valeur légale. Son format est basé sur la Décision (UE) 2018/646 du Parlement européen et du Conseil du 18 avril 2018 concernant un cadre commun pour l'offre de meilleurs services dans le domaine des aptitudes et des certifications (Europass) et abrogeant la décision n°2241/2004/CE.

© Union européenne, 2002-2020 | https://europa.eu/europass/en

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 règlementaires 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 règlementaires 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 (réusiner 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 disfonctionnements, 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, couts, 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,…).

4. Secteurs d'activité et/ou types d'emplois accessibles par le détenteur du certificat

Secteurs d'activité :

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'emploi accessible :

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.

Code(s) ROME :

M1801 - Administration de systèmes d''information
M1805 - Études et développement informatique

Références juridiques des 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).

5. Base officielle du certificat

Organisme(s) certificateur(s)

Nom légal certificateur(s) :
CONSERVATOIRE NATIONAL DES ARTS ET METIERS

Système de notation / conditions d'octroi

Modalités d'évaluation :
Les évaluations sont essentiellement organisées au plus proche des situations de travail du métier . Les épreuves sont conduites au travers les mises en situation, les études de cas, les travaux écrits et les présentations orales. Elles sont proposées sous des formes diverses (des travaux de groupes et individuels) facilitant l'inclusion des personnes en situation de handicap et permettant leur accompagnement tout au long de la préparation de la certification.
Les évaluations proposées sont :

- Evaluation écrite individuelle et/ou en groupe (2 à 4 personnes);
- Etude de cas pratiques;
- Epreuve individuelle orale;
- Dans le cadre d'un projet, élaboration des cahiers de test d'un composant informatique du SI ;
- Epreuves sous forme de travaux pratiques réalisées au moyen d'une plateforme de Cyber entrainement.

Description des modalités d'acquisition de la certification par capitalisation des blocs de compétences et/ou par correspondance :
La validation de la certification est conditionnée par la validation des 4 blocs communs et d'un bloc de spécialisation.

Niveau (national ou européen) du certificat

Niveau national (Décret n°2019-14 du 8 janvier 2019 relatif au cadre national des certifications professionnelles) : Niveau 6
Niveau du Cadre europeéen des certifications (CEC) : Niveau 6

Autorité responsable de l'habilitation

France compétences
6 rue du Général Audran 92400 Courbevoie

Accès au niveau suivant d'éducation / de formation

Accords internationaux de reconnaissance des qualifications

Base légale

Date de décision d'enregistrement : 21/12/2023
Durée de l'enregistrement : 5

Date d'échéance de l'enregistrement : 21/12/2028

6. Modes d'accès à la certification officiellement reconnus

Par expérience	Oui
En contrat de professionnalisation	Oui
Après un parcours de formation sous statut d'élève ou d'étudiant	Non
En contrat d'apprentissage	Oui
Par candidature individuelle	Non
Après un parcours de formation continue	Oui

7. Information complémentaire

Niveau d'entrée requis (Le cas échéant)

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).

Pour toute information complémentaire, notamment sur le système national de qualifications :

https://www.francecompetences.fr

National Europass Center

https://agence.erasmusplus.fr/programme-erasmus/outils/europass