Expert en architectures systèmes, réseaux et sécurité informatique

Prérequis d'inscription à la certification

- Les candidats doivent être titulaires d'une certification de niveau 6 (EU) ou d'un diplôme équivalent ou disposer d'une expérience professionnelle dans le domaine de plus de 2 ans.
- Procédure dérogatoire : Pour les candidats ne disposant pas d'un niveau de qualification suffisant ou issue d'un autre secteur, ces derniers peuvent accéder au parcours certifiant après avoir passé les tests d'inscription, rédigé une lettre de motivation et avoir effectué un entretien de sélection avec le responsable des admissions afin de valider leur pré-requis.

Les candidats doivent également :

- Avoir effectué une période en Entreprise (stage, alternance)
- Avoir remis les documents requis spécifiés dans le référentiel

Dans le cadre du respect du règlement de la certification, tout candidat peut saisir le référent handicap de INGETIS afin d'étudier les possibilités d'aménagement des modalités d'évaluation. Le référent handicap dispose de contacts et ressources afin d'analyser les besoins et mettre en œuvre les conditions matérielles nécessaires à la réalisation des évaluations. Sur conseil du référent handicap et dans le respect des spécifications du référentiel de la certification, le format de la modalité pourra être adapté si nécessaire.

Référentiel d'activités	Référentiel de compétences	Référentiel d'évaluation	
		Modalités d'évaluation	Critères d'évaluation
Bloc 1. Planifier et organiser un projet d'architecture systèmes et réseaux			
A1 Organisation du projet systèmes et réseaux			
A1.1 Analyse approfondie de l'architecture systèmes et réseaux existante	C1.1 **Réaliser l'audit des systèmes et réseaux informatiques existants de l'entreprise**, visant les performances des matériels, logiciels, réseaux et télécoms, en analysant l'utilisation des équipements et des applications, l'état des licences, la sécurisation de l'infrastructure, la sécurité du traitement des données et des sauvegardes, en interne et dans le cloud (ex. sécurité distribuée), en identifiant les risques potentiels les dysfonctionnements et les vulnérabilités, au niveau technique et du point de vue de la sécurité de fonctionnement, afin de cibler les besoins métier et d'outils informatiques, de proposer des préconisations d'évolution des technologies et des solutions techniques adaptées	C1.1 à C1.8 – Mise en situation professionnelle reconstituée, portant sur un projet d'architecture informatique optimisée et sécurisée. L'évaluation prendra la forme d'un dossier écrit et d'une présentation devant un jury composé de 2 professionnels minimum. Le candidat présente son projet pendant 20 mn devant le jury , suivi d'un entretien avec le jury de 20 mn sur le projet .	Ce1.1.1 L'audit technique inclut l'analyse approfondie des performances et de l'utilisation des équipements pour l'ensemble des infrastructures informatiques existantes. Il intègre une évaluation de la durabilité et de l'efficacité énergétique des équipements Ce1.1.2 L'audit de sécurité (interne, externe et cloud) permet d'analyser et de consigner des possibles dysfonctionnements et vulnérabilités visant le traitement des données, le fonctionnement et la sécurisation de l'infrastructure informatique. Il intègre l'évaluation des politiques de gestion des risques, la conformité réglementaire et le respect des normes de sécurité internationales. Il comprend une analyse des procédures de réponse aux incidents et de récupération après sinistre Ce1.1.3 Les résultats de l'audit de l'infrastructure informatique permettent de mettre en exergue les besoins métier, les performances souhaitées, ainsi que les préconisations d'évolution de l'infrastructure informatique
A1.2. Mise en place du plan de veille technologique et réglementaire des systèmes et réseaux informatiques	C1.2 **Concevoir un système de veille technologique et réglementaire visant l'architecture informatique**, en réalisant la collecte et l'analyse des tendances, évolutions, innovations, nouvelles méthodes, ainsi que des normes de conformité et des réglementations pour protéger les données, en utilisant des outils appropriés, afin de proposer les meilleurs services et solutions aux clients, en termes de systèmes, réseaux et sécurité informatique		Ce1.2.1 Le plan de veille technologique est conçu pour répondre aux objectifs du projet d'architecture informatique. Il intègre l'identification et l'analyse des tendances, innovations et réglementations émergentes. Ce1.2.2 La veille technologique s'appuie sur un ensemble d'outils (ex. Inoreader, Flipboard, etc.) et méthodes qui permettent de recueillir les informations utiles au projet d'architecture informatique (ex. référentiel de vulnérabilités) Ce1.2.3 L'analyse des informations issues de la veille technologique permet d'inclure des apports opérationnels et innovants à la solution d'architecture informatique

A.1.3 Analyse de faisabilité du projet d'architecture informatique	C1.3 **Réaliser l'étude de faisabilité du projet d'architecture informatique**, du point de vue technique, économique et opérationnel, en analysant les problématiques, les enjeux et le contexte de l'entreprise, ainsi que les risques et les contraintes, en recensant les exigences et les besoins applicatifs actuels et prospectifs, en prenant en compte la gestion des données selon le contexte, l'implantation et les spécificités du secteur d'activité de l'entreprise, afin de spécifier les conditions de nécessaires à la réussite du projet et l'avantage compétitif de l'entreprise		Ce1.3.1 Les besoins, l'environnement et les risques du projet d'architecture informatique sont correctement analysés Ce1.3.2 L'analyse des objectifs et du retroplanning du projet d'architecture informatique permettent de vérifier si la mise en place du plan du projet est possible Ce1.3.3 La faisabilité (économique, technique et opérationnelle) du projet d'architecture informatique est analysée par rapport au retour sur investissement du projet, et elle s'assure de l'alignement avec les objectifs de l'entreprise
A1.4 Description de la solution d'architecture informatique proposée à l'entreprise	C1.4 **Déterminer la solution informatique répondant aux besoins en systèmes et réseaux (ressources matérielles et logicielles)**, en utilisant les résultats de la veille technologique et concurrentielle, en sélectionnant les meilleures options par rapport aux problématiques techniques du projet de l'entreprise et les fonctionnalités attendues des utilisateurs, y compris en situation de handicap, en réduisant l'impact des équipements informatiques sur l'environnement, afin de proposer une architecture informatique optimisée, sécurisée et innovante		Ce1.4.1 La solution d'architecture informatique proposée répond aux problématiques techniques et aux fonctionnalités attendues des systèmes, réseaux et de sécurité informatique (différentes couches réseau, segmentation VLAN, microservices, API, interaction DBA…) Ce1.4.2 La solution d'architecture informatique prend en compte les résultats de la veille technologique et concurrentielle, et elle minimise l'impact sur l'environnement Ce1.4.3 La solution d'architecture informatique proposée répond aux besoins de tous les utilisateurs de l'entreprise, y compris ceux en situation de handicap, en intégrant des fonctionnalités d'accessibilité adaptées (comme des lecteurs d'écran, sous-titres, etc.)
A1.5 Élaboration du projet d'architecture informatique	C1.5 **Établir le plan du projet d'architecture informatique**, comportant un ensemble d'activités ordonnées dans le temps, en fonction des objectifs fixés pour les systèmes, réseaux et la sécurité informatique de l'entreprise, avec des budgets et des		Ce1.5.1 Les éléments du plan du projet d'architecture informatique sont clairement reliés à une méthodologie spécifique (ex. Agile, NetOps), et ils garantissent une approche structurée et adaptative pour la planification et l'exécution du projet.

	ressources associées (matérielles, technologiques, humaines), selon une méthodologie appropriée (ex. Agile), en utilisant des outils et logiciels de gestion de projet (ex. Jira, SAFe pour l'agilité à l'échelle), en vue d'assurer l'organisation opérationnelle du projet		Ce1.5.2 Le plan du projet d'architecture informatique comprend tous les éléments nécessaires à son fonctionnement (objectifs, tâches, étapes, budget, échéances, indicateurs de suivi, etc.) Ce1.5.3 La description du plan du projet d'architecture informatique permet son implémentation opérationnelle et s'insère dans le plan pluriannuel d'évolution de l'environnement
A1.6 Mise en œuvre du projet d'architecture informatique	C1.6 **Implémenter le projet d'architecture informatique**, dans un cadre qui facilite des méthodes de travail collaboratives de type fusion NetDevOps (Agile, NetOps, NetSecOps) entre plusieurs équipes de professionnels, permettant de créer des infrastructures souples et scalables, ainsi que l'automatisation des processus métier de bout en bout et l'intégration continue, en intégrant également de l'IA dans les systèmes, le deep-learning en cybersécurité, en coordonnant tous les éléments et les ressources (environnements, systèmes, plateformes, équipes informatiques), afin de garantir une infrastructure fiable, performante et sécurisée		Ce1.6.1 Le plan du projet d'architecture informatique est déployé selon la méthodologie choisie (ex. Agile, NetOps) Ce1.6.2 L'implémentation du plan du projet d'architecture informatique respecte le budget, la gestion établie des ressources, des risques et minimise l'impact sur l'environnement Ce1.6.3 Le plan du projet d'architecture informatique respecte les échéances, les normes associées aux objectifs définis tout en répondant aux exigences d'accessibilité pour les personnes en situation de handicap
A1.7 Evaluation de la performance du projet d'architecture informatique	C1.7 **Suivre le projet d'architecture informatique**, en observant l'évolution des résultats, suite à l'exécution du plan visant les systèmes, les réseaux et la sécurité informatique, en évaluant l'atteinte des objectifs du planning, le respect des budgets et des ressources allouées, par le biais d'indicateurs clé de performance (les KPI) et des outils de visualisation des données (reporting : QlikView, PowerBi), afin d'écarter les obstacles, d'assurer l'accompagnement au changement et d'identifier les axes de progrès		Ce1.7.1 Le suivi de l'évolution du projet d'architecture informatique est réalisé par le biais des indicateurs clefs de performance (KPI) définis Ce1.7.2 Les outils numériques utilisés permettent de mesurer l'efficacité et l'avancement du projet d'architecture informatique Ce1.7.3 L'analyse des informations issues de l'évaluation du projet d'architecture informatique permet d'identifier les axes d'amélioration
A1.8 Contrôle du projet d'architecture informatique	C1.8 **Superviser le projet d'architecture informatique**, en examinant la performance du projet, en mettant en place un plan d'amélioration de l'organigramme des activités prévues, en adaptant les objectifs et les		Ce1.8.1 L'identification des actions nécessitant des corrections permet d'actualiser le projet d'architecture informatique

	ressources du projet, en réduisant les latences, en assurant l'accompagnement au changement, afin de garantir la solution d'infrastructure informatique proposée et de répondre aux besoins de l'entreprise		Ce1.8.2 La résolution de problèmes permet de contrôler le projet d'architecture informatique par la définition des nouvelles tâches à réaliser Ce1.8.3 Les ajustements nécessaires au projet d'architecture informatique sont effectués en temps opportun, notamment en termes de calendrier et de réaffectation ou ajustement des ressources, et permettent de s'adapter aux évolutions du projet
Référentiel d'activités	**Référentiel de compétences**	**Référentiel d'évaluation**	
		Modalités d'évaluation	**Critères d'évaluation**
Bloc 2. Développer des solutions d'infrastructure systèmes et réseaux			
A2 Construire la solution technique du projet de systèmes-réseaux et sécurité			
A2.1 Élaboration de l'architecture informatique évolutive	C2.1 **Concevoir l'architecture informatique sécurisée de l'entreprise,** en choisissant ses spécificités (ex. classique, de cloud computing, hyperconvergée, infrastructure as a Service (IaaS)), visant l'ensemble des ressources matérielles (serveurs, routeurs, périphériques, etc.), logicielles (tels que CRM, ERP, messagerie), le service de stockage de données, les réseaux informatiques (tels que les accès à Internet, firewall, Wifi, antivirus) et télécoms, selon les besoins et les objectifs de l'entreprise, visant l'ensemble des opérations nécessaires, en fonction des exigences métier, en intégrant des objectifs RSE, en assurant l'accès aux personnes en situation de handicap, afin d'aligner la stratégie d'entreprise et les processus métier aux innovations technologiques	C2.1 à C2.7 – Mise en situation professionnelle reconstituée, sous forme de projet professionnel, portant sur la conception d'une architecture systèmes-réseaux sécurisée et innovante, et les outils associés. L'évaluation prendra la forme d'un dossier écrit et d'une présentation devant un jury composé de 2 professionnels minimum. Le candidat présente son projet pendant 20 mn devant le jury , suivi d'un entretien avec le jury de 20 mn sur le projet .	Ce2.1.1 L'architecture informatique répond aux besoins identifiés de l'entreprise en termes de systèmes et réseaux informatiques (ressources matérielles, stockage de données et télécoms) Ce2.1.2 L'élaboration de l'architecture informatique s'appuie sur les résultats de la veille technologique et réglementaire, et intègre des objectifs RSE Ce2.1.3 L'architecture informatique est conçue pour répondre aux objectifs de sécurité, aux contraintes réglementaires, et aux exigences métier de l'entreprise Ce2.1.4 L'architecture des systèmes et réseaux informatiques garantit une infrastructure inclusive et accessible à tous les utilisateurs, et elle répond aux exigences d'accessibilité des personnes en situation de handicap
A2.2 Mise en place de l'architecture informatique	C2.2 **Déployer l'architecture informatique de façon robuste et sécurisée de l'entreprise,** en provisionnant l'infrastructure (localement ou dans le cloud), le		Ce2.2.1 Le système d'exploitation, les systèmes virtuels et les applications dans le cloud, ainsi que les composantes réseaux et télécoms de l'architecture informatique sont mis

	réseau (configuration des routeurs, pares-feux, etc.), en paramétrant les accès aux comptes (messagerie électronique, base de données), en réalisant la gestion des configurations de manière uniforme et reproductible (Ansible), en automatisant et en standardisant les processus par le biais de l'infrastructure en tant que code (IaC), en utilisant la virtualisation, la containerisation et l'orchestration des conteneurs (ex. Kubernetes) afin de garantir flexibilité et évolutivité et en assurant les migrations, afin d'offrir une disponibilité et des performances maximale		en place de façon cohérente par rapport au plan de conception Ce2.2.2 L'architecture informatique présente un environnement d'exécution adapté des applications et un agencement optimisé entre les applications, le service de stockage et le réseau de l'entreprise Ce2.2.3 L'architecture informatique mise en place répond aux enjeux de disponibilité, performance, sécurité et automatisation des processus, notamment durant le déploiement (ex. plan de rollback) Ce2.2.4 L'architecture informatique mise en place permet l'accès aisé et sécurisé à l'ensemble des utilisateurs de l'entreprise, y compris en situation de handicap
A2.3 Maintenance du niveau de service optimal de l'infrastructure informatique	C2.3 **Coordonner la maintenance de l'architecture informatique**, visant la réduction des risques de pannes avant de se produire (maintenance préventive), l'identification et la correction des défaillances du système informatique lorsqu'ils surviennent et le rétablissement de l'état opérationnel (maintenance corrective), la mise à jour des applications ou du système et des correctifs (maintenance évolutive), en mettant en place un monitoring des systèmes et réseaux, en planifiant les interventions, en implémentant l'automatisation, en réalisant le support utilisateur, la sauvegarde de données, les scans antivirus et antimalware, les audits réguliers de performances et de sécurité, en réparant ou remplaçant des équipements endommagés, afin d'éviter ou de réduire le temps d'arrêt coûteux, le ralentissement des ordinateurs, logiciels et équipements réseau, et d'assurer le bon fonctionnement du matériel, des logiciels et des réseaux informatiques		Ce2.3.1 La maintenance préventive, corrective et évolutive permet d'identifier et corriger les défaillances de l'architecture informatique Ce2.3.2 Le monitoring des systèmes et réseaux permet une détection rapide des problèmes et d'assurer le support utilisateur adéquat Ce2.3.3 Les audits réguliers de performances et de sécurité permettent de maintenir le bon fonctionnement des équipements, des applications et des réseaux de l'entreprise Ce2.3.4 Les actions de maintenance impliquant l'automatisation permettent de réduire au maximum le temps d'arrêt et d'assurer un service optimal de l'architecture informatique, notamment avec une planification graduelle des opérations de maintenance (ex. Microsoft Intune)
A2.4 Surveillance du bon fonctionnement de l'infrastructure informatique	C2.4 **Piloter la supervision de l'architecture informatique,** visant la surveillance technique, applicative, le respect des engagements contractuels et des processus métiers de l'entreprise, en analysant		Ce2.4.1 La supervision de l'architecture informatique permet d'identifier correctement les éléments des systèmes et réseaux qui nécessitent une intervention (correctif, mise à jour, etc.)

	les écarts pour identifier les systèmes et applications qui ont besoin d'une mise à jour, d'une reconfiguration ou d'un correctif, en suivant le fonctionnement, les débits, la sécurité et le contrôle des flux des réseaux, en mettant en place un processus de contrôle des changements, en déterminant les mesures correctives, en définissant des alertes et des actions automatiques (ex. MEMOGuard), dans un cadre NetOps, en implémentant des solutions sur site et également ASP / SaaS, pour superviser à distance l'infrastructure, avec un monitoring AIOps (ex. ServiceNav), afin de garantir la fiabilité et la sécurité du système informatique		Ce2.4.2 Le processus de contrôle des changements permet d'apporter les mesures correctives de manière automatisée Ce2.4.3 La supervision de l'architecture informatique dans un cadre NetOps permet d'implémenter des solutions sur place et à distance Ce2.4.4 L'association du big data avec le machine learning et l'analyse en temps réel permet de garantir le fonctionnement et la sécurité de l'infrastructure informatique.
A2.5 Pilotage de l'amélioration de la qualité du service informatique	C2.5 **Organiser les actions d'amélioration de la qualité du service informatique**, en accélérant le déploiement et l'approvisionnement, en simplifiant les opérations par des logiciels fiables, en utilisant des processus automatisés, en contrôlant l'accès aux informations et la disponibilité des données des systèmes, en réduisant le délai de flux de données par des réseaux à faible latence et les coûts d'exploitation, en visant la haute disponibilité, en accélérant la mise à disposition des serveurs et en économisant de l'énergie par la virtualisation, en assurant la protection et la confidentialité des données et la cyber-résilience, en documentant les ressources, les configurations et les processus de manière détaillée, en augmentant l'efficacité du support aux utilisateurs et de la gestion du changement, afin de réduire les interruptions des opérations métier et d'assurer un fonctionnement optimal		Ce2.5.1 Les actions d'amélioration de la qualité du service informatique permettent de contrôler la disponibilité et la confidentialité des données Ce2.5.2 Les actions d'amélioration de la qualité du service informatique permettent d'augmenter le temps de disponibilité, de réduire les interruptions des opérations métier et les coûts d'exploitation Ce2.5.3 Les actions d'amélioration de la qualité du service informatique permettent d'assurer un support utilisateur adapté et efficace, et une adaptation continue aux besoins du public en situation de handicap Ce2.5.4 Les actions d'amélioration de la qualité du service informatique permettent d'économiser de l'énergie et de rester aligné à la démarche RSE de l'entreprise.
A2.6 Evolution de l'architecture informatique	C2.6 **Piloter l'évolution de l'architecture informatique**, en évaluant les tendances technologiques émergentes, en planifiant la mise en œuvre de l'évolution de l'architecture, en intégrant leur impact sur l'organisation du projet mis en œuvre, en anticipant les besoins futurs de l'architecture, en vérifiant ses effets sur l'orientation stratégique et éthique de l'entreprise, afin d'améliorer la résilience et la		Ce2.6.1 L'analyse et l'évaluation des tendances technologiques permet d'identifier les tendances technologiques émergentes pertinentes, nécessaires à l'évolution de l'architecture informatique Ce2.6.2 Les résultats de la veille permanente permettent d'identifier les technologies émergentes, qui seront utilisées dans le cadre de l'évolution de l'architecture informatique

	performance de l'architecture informatique sans compromettre sa stabilité opérationnelle		Ce2.6.3 L'intégration de technologies émergentes permet d'anticiper les besoins futurs et de guider la cohérence de l'alignement des évolutions avec les objectifs stratégiques et éthiques de l'entreprise Ce2.6.4 La mise en œuvre des plans élaborés, permet une amélioration mesurable de la performance de l'infrastructure et le maintien de sa stabilité opérationnelle Ce2.6.5 L'évaluation de la performance d'une intégration de technologies émergentes sur l'architecture existante permet d'identifier les domaines nécessitant des améliorations et des ajustements proactifs
A2.7 Elaboration de la documentation technique	C2.7 **Organiser la rédaction de la documentation technique de l'architecture informatique** (manuel utilisateur, guide d'utilisation), en décrivant l'architecture globale du réseau, le détail des composants du réseau, les systèmes et les solutions de gestion des données, l'utilisation de la virtualisation, les connectivités internes et externes, la gestion et la supervision, les procédures de maintenance et d'évolution, en français et en anglais, accompagnée d'un plan de formation des utilisateurs et en l'adaptant à la diversité du public et aux personnes présentant un handicap, afin d'assurer la résilience et les performances de l'infrastructure, tout en facilitant ses évolutions		Ce2.7.1 La documentation technique est complète et inclut l'ensemble des documents spécifiques visant : produits logiciels, système automatisé, solutions, matériel, maintenance, licences, contrats, fiches techniques, manuels, instructions, etc. Ce2.7.2 La documentation technique permet à son utilisateur une compréhension complète du fonctionnement de l'infrastructure systèmes et réseaux, de son utilisation et des évolutions possibles, en français et en anglais (équivalent niveau B2) Ce2.7.3 Le plan de formation intégré à la documentation technique permet à chaque type d'utilisateur d'avoir le niveau de compétences nécessaire à son utilisation Ce2.7.4 La documentation technique permet un accès aux utilisateurs en situation de handicap (ex. ISO 14289)

Référentiel d'activités	Référentiel de compétences	Référentiel d'évaluation	
		Modalités d'évaluation	Critères d'évaluation
Bloc 3. Piloter la sécurité de l'infrastructure informatique			
A3 Organiser la sécurité de l'infrastructure informatique			
A3.1 Evaluation de la sécurité existante des systèmes et réseaux informatiques	C3.1 **Réaliser l'état des lieux de la sécurité de l'infrastructure informatique et de la cybersécurité**, par rapport aux enjeux métiers, en effectuant des tests de sécurité, des audits sécurité (du site web, de l'infrastructure physique, des applications, des données, du cloud, de la messagerie), l'audit de conformité aux textes législatifs et réglementaires et l'audit de compromissions, afin d'identifier les vulnérabilités, les risques internes et externes de l'entreprise, et de définir les mesures de sécurité et les axes d'amélioration	C3.1 à C3.7 – Mise en situation professionnelle reconstituée portant sur la réalisation d'un projet de sécurité d'infrastructure informatique. L'évaluation prendra la forme d'un dossier écrit et d'une présentation devant un jury composé de 2 professionnels minimum. Le candidat présente son projet pendant 20 mn devant le jury , suivi d'un entretien avec le jury de 20 mn sur le projet .	Ce3.1.1 Les objectifs, le périmètre et les critères de l'audit de sécurité de l'infrastructure sont clairement définis Ce3.1.2 L'ensemble des tests (de charge, de panne, d'intrusion, de vulnérabilités) est réalisé de manière rigoureuse et méthodique et permet d'évaluer la robustesse de l'infrastructure face aux différents types de menaces Ce3.1.3 La conformité et le respect des obligations légales et réglementaires de l'infrastructure est vérifié de manière intégrale sur la base d'un référentiel adapté au projet (ex. ISO/CEI 27000, COBIT, méthodes EBIOS, Méhari, directives de l'ANSSI) Ce3.1.4 Le rapport de l'audit de sécurité inclut la synthèse fonctionnelle et opérationnelle de l'infrastructure, la liste des failles, le plan d'actions et les solutions possibles
A3.2 Mise en place du plan de veille de sécurité des systèmes et réseaux informatiques	C3.2 **Concevoir un système de veille lié à la sécurité de l'infrastructure informatique**, dans le cadre d'une approche d'amélioration continue, en conformité avec les normes et les référentiels applicables, en mettant en place une surveillance constante des évolutions et tendances en matière de sécurité informatique et de cybersécurité, des nouvelles technologies, des nouvelles failles de sécurité découvertes, afin d'anticiper les attaques, de limiter le risques d'incidents de sécurité et de proposer des solutions de sécurité adaptées et innovantes		Ce3.2.1 Le système de veille visant la sécurité de l'infrastructure informatique permet de surveiller constamment et de manière actualisée les nouvelles technologies et failles de sécurité identifiées Ce3.2.2 Le système de veille permet de garantir la conformité de l'infrastructure informatique aux normes et référentiels de sécurité en vigueur Ce3.2.3 Les résultats du système de veille lié à la sécurité de l'infrastructure informatique permettent de limiter les vulnérabilités de sécurité Ce3.2.4 Le système de veille permet d'identifier et de proposer des solutions de sécurité informatique et de cybersécurité adaptées et innovantes
A3.3 Construction de la politique de sécurité des	C3.3 **Définir la politique de sécurité de l'infrastructure informatique** et plus globalement, la politique de		Ce3.3.1 La politique de sécurité de l'infrastructure informatique couvre le périmètre et les enjeux stratégiques

systèmes et réseaux informatiques	sécurité des données dans l'entreprise (en local et dans le cloud), par rapport aux objectifs stratégiques de l'entreprise, visant le plan d'action, les objectifs de sécurité, les moyens, les mesures réalisables, l'accès aux données, la gestion des sauvegardes, la sécurisation des réseaux, des postes de travail et des données, les plans de continuité et de reprise d'activité en cas d'incident, afin de coordonner les actions de tous les acteurs pour assurer la sécurité du réseau et des données		des systèmes et réseaux (l'ensemble d'éléments à protéger), en termes de sécurité et cybersécurité Ce3.3.2 La politique de sécurité de l'infrastructure informatique est conforme aux lois, réglementations et standards applicables, et alignée avec les objectifs stratégiques de l'entreprise Ce3.3.3 La politique de sécurité de l'infrastructure informatique intègre la cartographie des risques par niveau de criticité et les mesures de sécurité informatique permettant de les traiter Ce3.3.4 La politique de sécurité de l'infrastructure informatique permet de coordonner les actions de tous les acteurs pour assurer la sécurité globale du réseau et des données
A3.4 Implémentation des solutions de sécurité des systèmes et réseaux informatiques	C3.4 **Mettre en œuvre des solutions de sécurité des systèmes et réseaux informatiques**, dans le cadre d'une approche innovante, prenant des formes spécifiques (ex. SIEM, DLP, IDS/IPS, etc.) et visant la sécurité d'accès (aux postes de travail, à distance, aux données), la sécurité des données, en lien avec la continuité des opérations et la sécurité physique, afin de garantir le niveau de sécurité nécessaire de l'infrastructure		Ce3.4.1 Les solutions mises en œuvre permettent de garantir la sécurité d'accès aux postes de travail, à distance, ainsi qu'aux données (ex. authentification, autorisation, pare-feu, VPN, détection d'intrusion, contrôle d'accès physique, standards pour le développement sécurisé) Ce3.4.2 Les solutions mises en œuvre permettent d'assurer la sécurité des données et leur intégrité contre tout type de menace ou vulnérabilité Ce3.4.3 Les solutions mises en œuvre permettent d'assurer un niveau adéquat de résilience des systèmes et réseaux en fonction de l'activité de l'entreprise (ex. ISO 22301) Ce3.4.4 Les solutions mises en œuvre sont en adéquation avec la sécurité physique et permettent une approche holistique de la sécurité de l'entreprise
A3.5 Détection des incidents de sécurité de l'infrastructure informatique	C3.5 **Mettre en place un système de détection des incidents de sécurité de l'infrastructure informatique (Security Operation Center - SOC),** en collaboration avec d'autres équipes, en utilisant un tableau de bord, des outils, des processus spécifiques et des dispositifs technologiques innovants (ex. SIEM, logiciels IDS et		Ce3.5.1 Le SOC est mis en place et est utilisé en collaboration avec des professionnels des équipes pertinentes de l'entreprise Ce3.5. 2 Le processus et les technologies employés pour la détection des incidents de sécurité de l'infrastructure

	EDR, scanner de vulnérabilité, machine learning), afin d'identifier le plus tôt possible les incidents de sécurité informatique, en minimisant les faux positifs et les faux négatifs, en évaluant et en priorisant les menaces potentielles, afin de réduire leurs impacts sur le fonctionnement de l'entreprise		informatique sont fonctionnels et adéquats par rapport aux contraintes et besoins de l'entreprise Ce3.5.3 Le système de détection des incidents de sécurité de l'infrastructure informatique mis en place permet un délai de réponse adéquat par rapport aux contraintes et besoins de l'entreprise Ce3.5.4 Le système de détection des incidents de sécurité de l'infrastructure informatique mis en place assure un niveau de détection et de priorisation des risques adéquats par rapport aux contraintes et besoins de l'entreprise
A3.6 Gestion des incidents de sécurité de l'infrastructure informatique	C3.6 **Organiser la gestion des incidents de sécurité et de cybersécurité de l'infrastructure** (ex. menace active, tentative d'intrusion, compromission réussie ou violation de données, etc.), en s'appuyant sur le système de détection et d'analyse des menaces ou des incidents de sécurité en temps réel, en coordonnant les équipes, en animant la cellule de crise, sur la base d'un plan et d'une stratégie à multiples facettes, afin de contrôler les risques de sécurité de l'infrastructure et d'assurer la continuité de l'activité de l'entreprise		Ce3.6.1 La gestion des incidents de sécurité et de cybersécurité de l'infrastructure informatique est mise en place selon une stratégie et un plan, adaptés aux besoins et aux particularités de l'entreprise Ce3.6.2 L'organisation de la gestion des incidents de sécurité et cybersécurité de l'infrastructure informatique mise en place permet d'assurer une réponse rapide / en temps réel, adaptée et proportionnée à la nature et à la gravité de l'incident Ce3.6.3 La cellule de crise est mise en place par des moyens proactifs et collaboratifs, qui permettent de contrôler les risques de sécurité de l'infrastructure Ce3.6.4 Les mesures et actions mises en place suite à un incident de sécurité et cybersécurité de l'infrastructure informatique permettent de garantir la continuité de l'activité
A3.7 Evolution de la politique et des solutions de sécurité de l'infrastructure informatique	C3.7 **Piloter les évolutions de la politique et des solutions de sécurité de l'infrastructure informatique**, en réalisant des audits réguliers, en suivant les indicateurs de performance, en s'appuyant sur la veille de sécurité de l'évolution des risques et des technologies de protection, et sur les apprentissages tirés des incidents passés, afin d'adapter les orientations stratégiques visant l'infrastructure de		Ce3.7.1 Les audits réguliers permettent d'identifier les améliorations potentielles et les vulnérabilités de la politique et des solutions actuelles de sécurité de l'infrastructure informatique Ce3.7.2 L'analyse des indicateurs de performance et de sécurité de l'infrastructure informatique permet d'adapter les objectifs de sécurité et les moyens nécessaires pour les atteindre

	l'entreprise, les objectifs de sécurité et les moyens nécessaires pour les atteindre, de limiter les dangers de sécurité et de responsabiliser les collaborateurs		Ce3.7.3 Les résultats de la veille de sécurité visant l'évolution des risques et les technologies de protection de l'infrastructure informatique permettent de guider et d'orienter les stratégies visant l'infrastructure de l'entreprise Ce3.7.4 Les apprentissages tirés des incidents passés permettent d'adapter les mesures de sécurité et de les affecter aux équipes qui en auront la responsabilité, de manière appropriée
Référentiel d'activités	**Référentiel de compétences**	**Référentiel d'évaluation**	
		Modalités d'évaluation	**Critères d'évaluation**
Bloc 4. Piloter l'équipe du projet d'architecture informatique			
A4 Management de l'équipe du projet d'architecture informatique			
A4.1 Définition des besoins en compétences de l'équipe du projet d'architecture informatique	C4.1 **Déterminer les compétences nécessaires à l'accomplissement du projet d'architecture informatique**, ainsi que les interactions prévues avec les autres équipes, en concordance avec les objectifs établis pour la solution proposée au client, en accord avec le cycle de vie du projet d'architecture informatique, en définissant les modalités afin de constituer une équipe projet performante	C4.1 à C4.6 – Mise en situation professionnelle reconstituée, portant sur le pilotage d'une équipe de projet d'architecture informatique. L'évaluation prendra la forme d'un dossier écrit et d'une présentation devant un jury composé de 2 professionnels minimum. Le candidat présente son projet pendant 20 mn devant le jury , suivi d'un entretien avec le jury de 20 mn sur le projet .	Ce4.1.1 Les compétences techniques et non techniques nécessaires sont identifiées par rapport aux objectifs et tâches figurant dans le plan du projet d'architecture informatique Ce4.1.2 Les rôles et responsabilités de chaque équipe sont détaillées Ce4.1.3 Les interactions de chaque profil au sein de l'équipe et avec les autres équipes sont reliées aux différentes étapes du projet d'architecture informatique (ex. RACI) Ce4.1.4 Les modalités d'accès et d'intégration des personnes en situation de handicap sont clairement définies, et les modalités de travail pour les membres de l'équipe en situation de handicap sont adaptées
A4.2 Création de l'équipe du projet de d'architecture informatique	C4.2 **Constituer l'équipe du projet d'architecture informatique**, par le biais de la formation interne et du recrutement, en collaboration avec l'équipe RH de l'entreprise, en identifiant les missions et les responsabilités associées à la solution d'architecture informatique, afin d'atteindre les objectifs du projet, fixés dans le cahier de charges		Ce4.2.1 Le plan de constitution de l'équipe, par recrutement et par formation interne, en collaboration avec les équipes RH, permet de couvrir l'ensemble des besoins identifiés en termes de compétences, d'expériences et d'aptitudes Ce4.2.2 Les descriptifs de poste permettent d'identifier les missions et responsabilités de chacun, et l'ensemble des tâches et responsabilités sont allouées

			Ce4.2.3 La stratégie d'intégration et d'adaptation mis en oeuvre pour les personnes en situation de handicap, incluant des aménagements spécifiques et une sensibilisation de l'équipe, leur permet de réaliser le travail dans des conditions satisfaisantes
A4.3 Gestion opérationnelle de l'équipe du projet de d'architecture informatique	C4.3 **Coordonner l'activité de l'équipe du projet d'architecture informatique**, par la gestion de l'intégration des nouveaux membres, en allouant les tâches et responsabilités et en veillant à l'équilibre des charges de travail, en français et en anglais selon les besoins, afin de garantir la productivité de l'équipe		Ce4.3.1 Le plan d'intégration des nouveaux membres est défini et permet une insertion efficace au sein de l'équipe Ce4.3.2 Le plan d'allocation des tâches et de gestion des ressources humaines permet une répartition équilibrée et efficace du travail Ce4.3.3 Le pilotage de l'équipe est réalisé en français ou en anglais, selon les besoins (équivalent niveau B2)
A4.4 Animation de l'équipe du projet d'architecture informatique	C4.4 **Accompagner les membres de l'équipe du projet d'architecture informatique**, en mettant en place des stratégies pour fluidiser la communication interne dans un contexte agile, les processus de développement et pour la résolution de problèmes, par le biais des échanges et des réunions spécifiques, en utilisant une plateforme collaborative inclusive et des outils numériques afin de faciliter la collaboration et la productivité de l'équipe		Ce4.4.1 La stratégie de communication au sein de l'équipe du projet de développement se réalise par des échanges réguliers en présentiel ou à distance, à travers des outils collaboratifs. Ce4.4.2 La résolution des problèmes au sein de l'équipe du projet d'architecture informatique par des réunions spécifiques permet d'améliorer le processus de travail et stimule la productivité Ce4.4.3 L'accompagnement des membres de l'équipe du projet d'architecture informatique (réunions, débriefings, etc.) facilitent l'engagement et l'avancée du projet Ce4.4.4 L'utilisation de plateformes, outils et modes de communication accessibles à tous les membres de l'équipe, y compris ceux en situation de handicap, permet de garantir une participation égale au sein d l'équipe
A4.5 Plan de formation de l'équipe du projet d'architecture informatique	C4.5 **Planifier la formation des membres de l'équipe du projet d'architecture informatique**, en mettant en place des actions de développement des compétences, afin d'acquérir, de maintenir et d'actualiser les compétences de l'équipe sur les avancées technologiques et méthodologiques, et afin de maintenir la performance de l'équipe projet et d'obtenir des résultats optimaux dans l'activité		Ce4.5.1 Les actions de formation individuelle et collective mises en place permettent d'acquérir, de maintenir et d'actualiser les compétences techniques et non techniques nécessaires au projet d'architecture informatique Ce4.5.2 Les actions de formation des membres des membres de l'équipe du projet d'architecture informatique prennent des formes variées (ex. en présentiel, e-learning, etc.) et favorisent la mise en situation

			Ce4.5.3 Les actions de formation présentent les aménagements nécessaires pour les personnes en situation de handicap, garantissant leur participation active Ce4.5.4 Le suivi de la performance collective et individuelle permet de s'assurer de l'efficacité des actions de formation
A4.6 Suivi de la performance de l'équipe du projet d'architecture informatique	C4.6 **Évaluer la performance de l'équipe du projet d'architecture informatique,** en établissant un référentiel de performance pour l'équipe et des référentiels de performance individuels, en analysant la performance collective et les performances individuels au regard de de ce référentiel, en réalisant des feedbacks réguliers et constructifs à double sens, en assurant des opportunités de développement au sein de l'équipe, et en établissant des plans de carrière en collaboration avec le service RH, afin d'optimiser la performance de l'équipe tout en assurant le bien-être des employés et en maintenant un environnement de travail positif et inclusif		Ce4.6.1 Les référentiels de performance sont adaptés au profils et niveau d'expérience des individus, et ils permettent de mesurer l'ensemble des dimensions nécessaires à la réussite du projet Ce4.6.2 L'analyse de la performance s'appuie sur des indicateurs objectifs, et elle intègre le suivi du bien-être au travail Ce4.6.3 Les feedbacks sont réguliers, constructifs, à double sens et structurés Ce4.6.4 Les plans de développement sont cohérents avec les plans de carrière, et ils assurent des opportunités de développement au sein de l'équipe à chacun Ce4.6.5 Les référentiels, la mesure de la performance, les plans de développements et les plans de carrière intègrent les aménagement nécessaires aux individus en situation de handicap

En complément de ces exigences, la certification implique la validation de deux compétences transversales :

- **"Maîtriser l'anglais technique dans son activité professionnelle"**: pour mener une veille technologique efficace et comprendre des informations techniques en anglais relatives à l'infrastructure systèmes et réseaux. En outre, un aspect crucial de cette compétence transversale est l'aptitude du candidat à communiquer en anglais dans un contexte professionnel. Cela inclut la capacité à participer à des discussions techniques, à présenter des concepts complexes et à collaborer efficacement avec des collègues et des partenaires internationaux. L'évaluation de cette compétence se fait à travers la capacité du candidat à rédiger un compte-rendu de veille technologique ou réglementaire en français à partir de sources anglophones et sa capacité à échanger en anglais dans un cadre professionnel.

- **"Intégrer les principes d'une économie verte et du numérique responsable dans le développement de projets informatiques"** : L'évaluation de cette compétence est établie par la capacité du candidat à appliquer les principes d'éco-conception dans le développement logiciel pour minimiser l'impact environnemental, tout en intégrant des pratiques de développement durable, comme l'optimisation des performances et l'utilisation efficiente des ressources.