5 - REFERENTIELS

Article L6113 Créé par LOI n°2018-771 du 5 septembre 2018 - art. 31 (V)
« Les certifications professionnelles enregistrées au répertoire national des certifications professionnelles permettent une validation des compétences et des connaissances acquises nécessaires à l'exercice d'activités professionnelles. Elles sont définies notamment par un référentiel d'activités qui décrit les situations de travail et les activités exercées, les métiers ou emplois visés, un référentiel de compétences qui identifie les compétences et les connaissances, y compris transversales, qui en découlent et un référentiel d'évaluation qui définit les critères et les modalités d'évaluation des acquis. »

Candidat en situation de handicap :
Dans le cadre du respect du règlement de la certification, tout candidat peut saisir le référent handicap (présent sur chaque site de formation d'IEF2i) 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 aménagements 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 adaptée si nécessaire. L'ingénieur de certification s'engage dans la mesure du possible à élaborer des modalités d'évaluation inclusives permettant une adaptation du format.

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compristransversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
MODELISER UNE INFRASTRUCTURE SYSTEMES, RESEAUX SECURISEE ET RESPECTUEUSE DE LA POLITIQUE RSE **A1. Audit et tests des systèmes et réseaux de l'organisation** : - Les postes fixes : ordinateurs fixes, unités centrales et leurs accessoires. - Les postes mobiles : ordinateurs portables, tablettes, smartphones. - Les périphériques : imprimantes, disques durs externes, caméras, micros. - Les espaces de stockage : Cloud, serveur. - Les réseaux : Bluetooth, wifi, modems. - Les logiciels, applications et leurs licences. - Utilisation d'outils adaptés (GLPI). - Collaboration avec les équipes informatiques ou utilisateurs concernés et prise en compte des situations de handicap (respect du référentiel RGAA notamment).	**C1.** Réaliser un inventaire et des tests des systèmes et réseaux de l'organisation en se basant sur une méthodologie d'audit et des outils adaptés afin de déterminer et analyser les modes d'utilisation des systèmes et réseaux par les parties prenantes internes et externes de son entreprise.	**Evaluation n°1 -** **Mise en situation professionnelle** **(C1 à C9)** Toutes les compétences du bloc sont évaluées selon la production suivante. **Proposition d'une architecture systèmes et réseaux adaptée aux attentes des besoins de l'entreprise.** Le candidat travaillera sur un cas réel qu'il fera valider préalablement par un tuteur. - Production : Le candidat devra réaliser et présenter au jury un rapport d'audit du réseau et du système informatique d'une entreprise ainsi qu'une proposition d'architecture système et réseau adapté aux attentes de l'entreprise. - Soutenance orale : Le candidat présentera oralement son rapport	**C1 : Evaluation des points suivants :** • L'inventaire des systèmes et réseaux est réalisé de façon claire et exhaustive via un outil de gestion des services informatiques. • Sont inventoriés : les postes fixes, les postes mobiles, les périphériques, les espaces de stockage, les réseaux, les logiciels. • La méthode utilisée et les outils mobilisés sont précisés et justifiés. • Toutes les parties prenantes sont prises en compte (internes et externes) ainsi que les situations de handicap (respect du référentiel RGAA notamment) ; • Le programme de tests est cohérent.

A2. Recueil et analyse des besoins et comportements des parties prenantes en matière de système et réseaux prenant en compte : - Le contexte, - Les situations de handicap, - Les enjeux, - Les objectifs, - Les contraintes du SI, - Réglementation en matière de sécurisation (référentiel général d'interopérabilité (RGI), référentiel général de sécurité (RGS), RGPD,…), cybersécurité (textes législatifs et réglementaires de niveau national, OTAN et UE), éthique, green IT, prise en compte des situations de handicap.	**C2.** Recueillir les besoins exprimés par les parties prenantes en se basant sur le contexte, les enjeux, les objectifs et contraintes du SI afin d'identifier leurs besoins informatiques. **C3.** Analyser les attentes fonctionnelles des utilisateurs de réseaux informatiques internes et externes, en vue d'orienter la recherche d'une infrastructure adaptée aux besoins et respectueuse de la politique RSE et de sécurisation informatique de l'entreprise.	devant un jury. Ce rapport aura été remis préalablement au jury pour le passage de sa soutenance.	**C2-C3 : Evaluation des points suivants :** • Les besoins exprimés par les parties prenantes sont recueillis et analysés. • Le contexte, les enjeux, les objectifs, les situations de handicap et les contraintes SI sont pris en compte dans la recherche d'une infrastructure informatique adaptée.
A3. Définition de l'infrastructure informatique adaptée aux besoins et aux contraintes définis en amont du projet : - Cartographie du système d'information - Définition des outils nécessaires au bon fonctionnement des infrastructures informatiques ; - Veille technologique et réglementaire (mises à jour, mises hors service, montées de version des serveurs et des logiciels, IA, Data science, IOT,…) et réglementaire	**C4.** Cartographier le système d'information en précisant les technologies, la nature et le dimensionnement des liens réseaux et les systèmes afin de déployer une infrastructure informatique adaptée, sécurisée en conformité avec la politique RSE de l'organisation. **C5.** Définir les outils nécessaires au bon fonctionnement de l'infrastructure informatique en effectuant une veille réglementaire en matière de sécurisation informatique et technologique des matériels, logiciels et systèmes utiles à l'optimisation des systèmes et réseaux afin de proposer des améliorations à l'infrastructure systèmes et réseaux.		**C4-C5 : Evaluation des points suivants :** • Le système d'information est cartographié. • La cartographie de l'infrastructure informatique précise les technologies, la nature et le dimensionnement des liens réseaux et les systèmes. • Les outils nécessaires au bon fonctionnement de l'infrastructure sont définis. • Des veilles réglementaire et technologique sont démontrées (mises à jour, mises hors service,

(RGPD, DSA[1], DMA, règles de sécurisation informatique, etc.) - Propositions d'investissements informatiques.			montées de version des serveurs et des logiciels, IA, Data science, IOT,…). • Des propositions d'investissements informatiques sont formulées et sont conformes à la politique RSE de l'entreprise.
A4. Formalisation des supports techniques et des procédures de configuration et d'exploitation dématérialisés et automatisés de l'infrastructure systèmes et réseaux : - Définition du schéma général des connexions ; - Intégration des possibilités d'évolution ; - Transition écologique et numérique ; - Respect des normes en vigueur en matière de sécurité du SI, RGPD cybersécurité. - Prise en compte des situations de handicap (adaptation du format).	**C6.** Rédiger les supports techniques et des processus dématérialisés et automatisés en s'appuyant sur la définition du schéma général des connexions, de l'intégration des possibilités d'évolution, des situations de handicap ainsi que la réglementation en vigueur en matière de sécurisation pour garantir l'adaptation du format, les performances et la qualité de l'infrastructure informatique (pannes, flux, disponibilité des systèmes) et la transition écologique et numérique.		**C6 : Evaluation des points suivants :** • Les supports techniques précisent et organisent les processus ainsi que les modes opératoires de mise en production, déploiement, administration et maintenance. • Les supports techniques mettent en évidence la définition du schéma général des connexions, de l'intégration des possibilités d'évolution, des situations de handicap ainsi que la réglementation en vigueur en matière de sécurisation.
A5. Rédaction du cahier des charges du projet d'infrastructure systèmes et réseaux : - Cartographie des ressources existantes (architectures	**C7.** Rédiger le cahier des charges du projet d'infrastructure en analysant le contexte du projet d'infrastructure systèmes et réseaux, en cartographiant les ressources existantes de l'infrastructure afin de proposer une		**C7 : Evaluation des points suivants :** • Les spécifications techniques sont complètes. • La structure du cahier des charges est

[1] Le futur règlement DSA (pour Digital Services Act) est, avec le règlement sur les marchés numériques (DMA), un des grands chantiers numériques de l'Union européenne (UE). Présenté fin 2020 par la Commission européenne, il a été définitivement voté par le Parlement européen le 05 juillet 2022.

systèmes et réseaux existantes) ; - Identification des contraintes (matérielles, logicielles, économiques, humaines, planning) et des opportunités ;	infrastructure système et réseaux prenant en compte toutes les contraintes identifiées et les opportunités du projet et adaptés aux besoins exprimés par toutes les parties prenantes.		conforme. • Le contenu du cahier des charges est détaillé. • Le cadre financier applicable est précisé.
- Analyse des risques techniques (stabilité électrique, débit, surcharge, compatibilité matériel…) ;	**C8.** Analyser les risques techniques et contraintes associés au projet de l'infrastructure en se basant sur la stabilité électrique, sur le débit, la surcharge et la compatibilité des matériels afin d'envisager les solutions préventives dans le cadre du projet d'ingénierie systèmes et réseaux sécurisé.		**C8 : Evaluation des points suivants :** • Les risques techniques et contraintes de la structure sont analysés et s'appuient sur les critères suivants : • Stabilité électrique • Débit • Surcharge • Compatibilité des matériels • Cybersécurité.
- Formalisation des besoins métiers exprimés en demandes fonctionnelles et techniques en prenant en compte des situations de handicap et la transition écologique et numérique.	**C9.** Formaliser les besoins métiers exprimés en demandes fonctionnelles et techniques en prenant en compte les situations de handicap et transition écologique et numérique afin de les rendre exploitables par l'équipe de déploiement de l'infrastructure systèmes et réseaux.		**C9 : Evaluation des points suivants :** • Les besoins métiers exprimés sont formalisés en demandes fonctionnelles et techniques. • Les situations de handicap sont prises en compte par l'équipe en charge du déploiement de l'infrastructure systèmes et réseaux. • Les contraintes réglementaires sont mises en évidence (règles de sécurisation du SI, RGPD, cybersécurité, Green IT).

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activitésexercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compristransversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
DEPLOYER ET ADMINISTRER UNE INFRASTRUCTURE SYSTEMES ET RESEAUX SECURISEE **A6. Conception du plan de déploiement de l'infrastructure système et réseaux retenue par l'entreprise :** - Identification des différentes étapes du déploiement ; - Conception du plan de transition dans le cadre d'un projet de migration ; - Synthèse des ressources matériels et humains nécessaires en prenant en compte les situations de handicap ; - Planification du déploiement des matériels et logiciels ; - Définition des indicateurs de contrôle de suivi du déploiement.	**C10.** Concevoir le plan de déploiement de l'infrastructure système et réseaux retenue par l'entreprise reposant sur la planification du déploiement des matériels et logiciels, la conception du plan de transition le cas échéant, la synthèse des ressources nécessaires, la définition des indicateurs de contrôle dans le but de garantir le respect du cahier des charges.	**Evaluation n°2 :** **C10 à C15 -** **Mise en situation professionnelle** Toutes les compétences du bloc sont évaluées selon la production suivante. **Déploiement et administration d'une infrastructure systèmes, réseaux sécurisée.** Le candidat travaillera sur un cas réel qu'il fera valider préalablement par un tuteur. - *Production :* Le candidat devra réaliser et présenter au jury un plan de déploiement d'infrastructure systèmes et réseaux, dans le respect des normes de sécurité, pour une organisation. - *Soutenance orale :* Le candidat doit présenter un	**C10 : Evaluation des points suivants :** • Les différentes étapes du déploiement sont identifiées. • Le plan de transition est présenté dans le cadre d'un projet de migration. • Les ressources matériels et humains nécessaires en prenant en compte les situations de handicap sont répertoriées. • Le déploiement des matériels et logiciels est planifié. • Les indicateurs de contrôle de suivi du déploiement sont définis. **C11 : Evaluation des points suivants :** • Le retroplanning du plan de déploiement de l'infrastructure système et réseaux est présenté aux parties prenantes.
A7. Présentation aux utilisateurs de l'impact organisationnel de la nouvelle infrastructure informatique.	**C11.** Planifier les phases d'installation des réseaux et systèmes, en concertation avec les parties prenantes, afin d'assurer leur bonne information sur les nouvelles fonctionnalités disponibles et l'impact organisationnel de la nouvelle infrastructure réseaux et systèmes.		

A8. Configuration d'une infrastructure systèmes et réseaux hybride performante et sécurisée mobilisant : - Des techniques de redondance et d'interconnexion des réseaux. - Une infrastructure systèmes et réseaux ouverte vers l'extérieur (cloud, VPN,…). - La maîtrise des règles de sécurité informatique en vigueur. **A9. Paramétrage des serveurs et des routeurs** : - incluant les services de sécurité (firewalls, VPN, Mobile Device Management, Active Directory, Authentification multifacteur, Bastion hosts…) ; - Respectant la réglementation en vigueur (Règles de sécurité informatique, RGPD, etc.). **A10. Administration des droits d'accès des données en réseau hétérogène en mode multisites (machines, utilisateurs) et gestion des comptes sur site et dans le cloud (IAM, gestion globale des identités).**	**C12.** Configurer une infrastructure systèmes et réseaux hybride en mobilisation les techniques de redondance, d'interconnexion, cloud ainsi que la réglementation en matière de sécurité en vigueur afin de garantir les performances et la sécurité des systèmes et réseaux interconnectés. **C13.** Paramétrer les dispositifs réseaux (serveurs, routeurs incluant les services de sécurité), prenant en compte le type d'accès aux ressources dans le périmètre de l'entreprise ou dans le cloud public, afin d'installer et de configurer les postes utilisateurs conformes aux besoins. **C14.** Paramétrer les machines et les habilitations des utilisateurs en termes d'accès et de partages sur site et dans le cloud en s'assurant de la conformité des installations vis-à-vis du cahier des charges et des règles de sécurité de l'entreprise afin de garantir une infrastructure fonctionnelle et sécurisée.	rapport de mission qui aura été remis préalablement au jury pour le passage de sa soutenance. Le candidat présentera oralement son projet devant un jury.	• Présentation des nouvelles fonctionnalités. • Les impacts organisationnels de la nouvelle infrastructure informatique sont détaillés. **C12 : Evaluation des points suivants :** • Les techniques de redondance et d'interconnexion des réseaux sont maîtrisées. • Les clouds public et privé sont connus. • Les règles de sécurité informatique en vigueur sont présentées. **C13 : Evaluation des points suivants :** • Le paramétrage est conforme au cahier des charges. • Les accès aux bases de données sont définis et sont conformes à l'organisation de l'entreprise. **C14 : Evaluation des points suivants :** • Le type d'accès aux ressources est pris en compte dans le paramétrage des serveurs et routeurs (machines, utilisateurs, IAM, gestion

A11. Paramétrage des pare-feux : - Définition de la cartographie des zones de sensibilité aux risques ; - Adaptation des systèmes d'alarme et protections aux niveaux de risques ; - Intégration au système d'information ; - Pilotage des procédures de contrôles des pare-feux.	**C15.** Paramétrer les pare-feux en délimitant des zones de sensibilité à l'aide d'une cartographie pour concevoir et mettre en œuvre des systèmes d'alarmes et de protection intégrés au système d'information.		globale des identités). • Les serveurs et routeurs sont configurés dans le respect de la réglementation en vigueur (Règles de sécurité informatique, RGPD, cybersécurité). **C15 : Evaluation des points suivants :** • La cartographie des zones de sensibilité aux risques est établie ; • Les systèmes d'alarme et protections sont adaptés aux niveaux de risque ; • L'intégration au système d'information est correcte ; • Une procédure de contrôle des pare-feux est explicitée.

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activitésexercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compristransversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
ASSURER LA MAINTENANCE D'UNE INFRASTRUCTURE SYSTEMES ET RESEAUX SECURISES **A12. Sécurisation des données des systèmes et réseaux :** - Identification des différentes catégories d'utilisateurs ; - Définition du format des données ; - Gestion du maintien en condition opérationnelle et de sécurité des infrastructures systèmes et réseaux (gestion des mises à jour, sauvegardes, incidents et conformité des configurations) - Maintien des solutions de stockage et sauvegarde ; - Mise en œuvre des dispositifs de protection et de sécurisation ; - Conformité des accès au regard de l'organisation de l'entreprise ; - Respect des contraintes liées à la réglementation en vigueur (Règles de sécurité informatique, RGPD) ; - Veille technologique et réglementaire ; - Prise en compte des recommandations de l'ANSSI ;	**C16.** Définir les différentes catégories d'utilisateurs, conformément au cahier des charge et à la réglementation en vigueur en matière de sécurisation des données, et du format des données afin de sécuriser la gestion du dimensionnement des espaces de stockage et de sauvegarde des données, des comptes et des accès réseaux.	**Evaluation n°3 :** **C16 à C24 :** **Mise en situation professionnelle** Toutes les compétences du bloc sont évaluées selon la production suivante. **Maintenance d'une infrastructure systèmes et réseaux.** Le candidat travaillera sur un cas réel ou fictif. - *Production :* Le candidat devra rédiger un programme de maintenance et d'entretien d'une infrastructure systèmes et réseaux sécurisée. - *Soutenance orale :* Le candidat doit présenter devant un jury son programme de maintenance et d'entretien d'une infrastructure systèmes et	**C16 : Evaluation des points suivants :** • Les différentes catégories d'utilisateurs sont identifiées. • Le format des données est adapté à la structure des espaces de stockage et de sauvegarde. • Le dimensionnement des espaces de stockage et de sauvegarde est présenté. • Le maintien en condition opérationnelle et de sécurité des infrastructures systèmes et réseaux est démontrée par les critères suivants : o Gestion des mises à jour ; o Gestion des sauvegardes ; o Gestion des incidents ; o Conformité des configurations. • Le choix des dispositifs de protection et de sécurisation sont argumentés. • Le respect du cahier des charges et la conformité des accès au regard de

- Respect du cahier des charges.		réseaux sécurisée qui aura été remis préalablement au jury pour le passage de sa soutenance.	l'organisation de l'entreprise sont démontrés. • Le respect des contraintes liées à la réglementation en vigueur (Règles de sécurité informatique, RGPD) ainsi la prise en compte des recommandations de l'ANSSI sont démontrés.
A13. Identification des risques associés à l'infrastructure informatique : - Maîtrise des différents types de rupture de charge ; - Identification des menaces d'intrusion (IDS/IPS) - Mise en œuvre d'alertes.	**C17.** Identifier les risques associés à l'infrastructure en se basant sur les possibilités ruptures de charges, les menaces d'intrusion afin de mettre en œuvre des alertes utiles à la surveillance des systèmes et réseaux.		**C17 : Evaluation des points suivants :** • Les différents types de rupture de charge sont maîtrisés. • En cas de menace d'intrusion, un plan d'actions de crise est mis en œuvre. • Des alertes sont configurées.
A14. Accompagnement et communication aux utilisateurs de l'infrastructure systèmes et réseaux : - Implication des utilisateurs ; - Prise en compte des situations de handicap (respect du référentiel RGAA notamment) - Mise à jour des supports ; d'information et mise à disposition des utilisateurs ; - Définition d'une liste d'interlocuteurs à prévenir ; - Préparation des mailings-types et des procédures de gestion de crises.	**C18.** Communiquer aux utilisateurs la mise à jour des supports d'information et des procédures de gestion de crise en se basant sur une liste d'interlocuteurs définie et des mailings-types préparés en amont selon le niveau de crise afin de les impliquer dans la démarche de sécurisation de l'infrastructure système et réseaux de l'organisation. **C19.** Définir le plan d'action à mettre en œuvre selon chaque niveau d'alerte en établissant une échelle de niveaux de crise afin de formuler une réponse coordonnées aux alertes sur l'infrastructure.		**C18-C21 : Evaluation des points suivants :** • Les procédures de gestion de crises sont communiquées aux utilisateurs. • Les situations de handicap sont prises en compte dans les moyens de communication utilisés à destination des utilisateurs. • Les supports d'information sont mis à disposition des utilisateurs.

A15. Définition des niveaux d'alerte et traitement des tickets : - Diagnostic ; - Rapport d'intervention ; - Mise en conformité de l'infrastructure.	**C20.** Organiser le traitement des demandes utilisateurs et les alertes formulées sous la forme de tickets générés dans un outil dédié, selon un ordre de priorité défini, afin de résoudre les dysfonctionnements et les possibles dommages. **C21.** Assurer les mises à jour, mises hors service, et montées de version des serveurs en accord avec les règles définies par la Direction du Système d'Information concerné.		• Une liste d'interlocuteurs à prévenir en cas de crise est définie. • Les mailings-types sont préparés en fonction du niveau d'alerte.
A16. Organisation de la maintenance de l'infrastructure réseaux et systèmes : - Gestion du parc informatique (maintien de l'inventaire des actifs à jour) et des composants de l'infrastructure ; - Organisation des tests nécessaires à la vérification de la conformité du paramétrage défini ; - Elaboration d'une trame d'audit interne ;	**C22.** Planifier les phases de test de l'infrastructure réseaux et systèmes, en impliquant les utilisateurs et en maîtrisant les méthodes de tests de mesure de la performance de réseaux et systèmes, dans le but de recenser les anomalies et d'apporter les améliorations nécessaires.		**C22 : Evaluation des points suivants :** • L'inventaire du parc informatique est à jour (inventaire des actifs et composants de l'infrastructure informatique (réseaux LAN et WAN, serveurs virtuels, stockages, hôtes, châssis). • Le pilotage des sauvegardes est démontré par la définition de la fréquence des sauvegardes et par les supports de sauvegarde présentés.
A17. Pilotage des opérations de sauvegarde des sources d'installation, les licences et les fichiers de configuration des applications : - Chiffrement des données avant sauvegarde ;	**C23.** Définir les supports et la fréquence des sauvegardes en lien avec le volume de données numériques produites sur un temps donné conformes aux dispositifs juridiques de protection et de conservation des données et en s'appuyant sur des sauvegardes en ligne et des sauvegardes déconnectées afin de		**C23 : Evaluation des points suivants :** • Les sources d'installation, les licences et les fichiers de configuration des applications sont identifiées et planifiées

- Définition des supports de sauvegarde ; - Respect des dispositifs juridiques de protection et de conservation des données.	permettre une restauration plus rapide des activités opérationnelles en cas d'incident, notamment en cas de cyberattaque.		dans les opérations de sauvegarde. • Le chiffrement des données est mis en œuvre avant sauvegarde. • Les supports de sauvegarde sont définis et sont argumentées (sauvegardes en ligne, déconnectées).
A18. Gestion inclusive de l'équipe de maintenance des systèmes et réseaux sécurisés : - Mise en œuvre de la culture DevOps ; - Prise en compte des situations de handicap dans la définition des rôles de chacun et la répartition des missions ; - Maîtrise des méthodes de tests de mesure de performance de réseaux et systèmes ; - Planification des interventions de l'équipe de maintenance réseaux et systèmes - Recensement des anomalies ; - Description des améliorations apportées.	**C24.** Mobiliser les techniques et outils de conduite de projets inclusifs en mobilisant la culture DevOps et les méthodes de tests de mesure de performance afin de produire les livrables du projet d'infrastructure informatique dans le temps imparti, au niveau de qualité et de sécurité attendu.		**C24 : Evaluation des points suivants :** • Les opérations de maintenance sur le matériel et les logiciels sont planifiées. • Les tests nécessaires à la vérification de la conformité du paramétrage défini est organisé. • Les anomalies sont recensées et des propositions d'améliorations sont présentées de façon argumentée.

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activitésexercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compristransversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
OPTIMISER LA PERFORMANCE DES SYSTEMES ET RESEAUX INFORMATIQUES SECURISES **A19. Définition des critères de mesure de la performance des systèmes et réseaux informatiques sécurisés :** - Définition des indicateurs de niveaux de performance des réseaux et systèmes ; - Choix des référentiels théoriques ; - Respect de la règlementation en matière de sécurisation des infrastructures et de cybersécurité ; - Suivi et création de compteurs et suivi de performance, création de scénarii et d'alertes de performance ; - Mise en œuvre de scenarios utilisateurs pour un contrôle des performances de bout en bout.	**C25.** Sélectionner des indicateurs de mesure de la performance de réseaux et systèmes en définissant des référentiels théoriques dans le but de créer des outils de mesure des performances de réseaux et des systèmes sécurisés. **C26.** Enregistrer l'activité déployée sur les systèmes et réseaux en se basant sur la définition des différentes catégories d'utilisateurs, des utilisations programmées et des zones de déperdition identifiées, en vue de mesurer les niveaux de performance et repérer les limites structurelles l'infrastructure informatique et des matériels. **C27.** Analyser l'activité réseaux en se basant sur les analyses des utilisations non programmées afin de repérer les limites structurelles de l'architecture et des matériels et ainsi proposer des scénarii et des alertes de performance.	**Evaluation n°4 :** C25 à C34 : **Mise en situation professionnelle** Toutes les compétences du bloc sont évaluées selon la production suivante. **Le candidat devra proposer des pistes d'amélioration de la performance des réseaux et systèmes d'entreprise.** - Production : A partir d'un cas réel ou fictif, le candidat devra proposer : - un état des lieux des mesures de performance des systèmes et réseaux ; - une priorisation des projets, - une capitalisation sur les dysfonctionnements ; - des mesures permettant d'améliorer la performance ; - une veille technologique.	**C25 : Evaluation des points suivants :** • Les indicateurs des niveaux de performance sont définis. • Les référentiels théoriques choisis sont justifiés. **C26-C27 : Evaluation des points suivants :** • Les catégories d'utilisateurs sont présentées. • Des compteurs de performance sont présentés. • Les résultats des mesures de performance sont correctement présentés et analysés. • Les zones de déperdition sont

		- Soutenance orale : Le candidat présentera oralement son projet devant un jury.	identifiées. • Les capacités limites de l'infrastructure sont évaluées. • Des propositions de scenarii et alerte de performance sont présentées.
A20. Analyse des utilisations programmées et non programmées : - Présentation et analyse des résultats des mesures ; - Implication des utilisateurs ; - Identification des zones de déperdition ; - Evaluation des capacités limites.	**C28.** Tester la réaction des systèmes et des réseaux lors de sollicitations spécifiques adaptés à l'analyse des risques de saturation et de rupture, en mettant en œuvre des tests spécifiques et en produisant des rapports de mesures, afin d'évaluer les risques de saturation et de rupture de l'activité.		**C28 : Evaluation des points suivants :** • Les tests spécifiques sont adaptés à l'analyse des risques de saturation et de rupture. • Le rapport de mesures est complet et précis. • L'analyse est rapportée au cahier des charges.
A21. Analyse et contrôle des risques de saturation : - Veilles technologique et réglementaire ; - Mise en œuvre de tests spécifiques, adaptés à l'analyse des risques de saturation et de rupture ; - Production de rapport de mesures ; - Mise en regard avec le cahier des charges.	**C29.** Exercer une veille technologique et réglementaire sur les solutions réseaux en évaluant et comparant les solutions de réparation dans le but de rechercher et analyser les possibilités d'amélioration d'architectures. **C30.** Présenter des projets d'amélioration des solutions réseaux, en estimant les coûts et délais d'intervention, dans le but d'anticiper sur les développements nécessaires.		**C29 et C30 : Evaluation des points suivants :** • La méthodologie de veille est mise en œuvre et présentée. • Les solutions de réparation de zones de réseaux sont évaluées et comparées. • Les conditions de mise en place d'axes d'amélioration sont analysées et explicitées.

A22. Etude des solutions d'optimisation des systèmes et des réseaux sécurisés : - Mise en œuvre d'une veille technologique et réglementaire ; - Evaluation et comparaison des solutions de segmentation des zones réseaux ; - Analyse des conditions et impacts de mise en place d'axes d'amélioration ;	**C31.** Planifier les interventions d'amélioration sur les systèmes et réseaux en évaluant et comparant les solutions de segmentation des zones réseau, en analysant les possibilités d'optimisation en concertation avec les parties prenantes, en décrivant les risques éventuels de modifications, en définissant les coûts et les délais afin de garantir la continuité d'activité.		**C31 : Evaluation des points suivants :** • Les possibilités d'optimisation des performances de réseaux sont justifiées. • Des veilles technologiques et réglementaires sont illustrées. • Les risques éventuels de modification de réseaux sont détaillés.
A23. Gestion et planification des interventions sur l'infrastructure informatique : - Animation d'équipe de techniciens informatiques selon la culture DevOps ; - Prise en compte des situations de handicap dans la définition des rôles de chacun et la répartition des missions ; - Maîtrise de la technique de gestion de projet ; - Analyse des possibilités d'optimisation des performances ; - Description des risques éventuels de modification de réseaux ; - Définition des coûts et délais d'intervention ; - Planification du programme des interventions.	**C32.** Animer l'équipe de techniciens informatiques en s'appuyant sur la culture DevOps, en prenant en compte les situations de handicap et en maîtrisant les techniques de base de la gestion de projet afin de planifier le programme des interventions sur l'infrastructure informatique.		**C32 : Evaluation des points suivants :** • La gestion d'équipe de techniciens est démontrée par la planification des tâches, la répartition des tickets et le recours à la méthodologie de gestion de projet agile ancrée dans la culture DevOps. • Les coûts et délais d'intervention sont précisés. • Le programme des interventions est établi.

A24. Anticipation des risques de défaillance des systèmes et réseaux : - Analyses proactives et réactives des causes d'incidents ; - Mise en place des alertes et dispositifs de prévention ; - Formation des utilisateurs à la détection des pannes ; - Adaptation du dimensionnement des alimentations de secours ; - Mise en œuvre de la continuité des systèmes et réseaux (PRA/PCR).	**C33.** Anticiper les risques d'incidents sur les systèmes et réseaux en effectuant des analyses proactives et réactives, en formant les utilisateurs à la détection des pannes et en adaptant le dimensionnement des alimentations de secours dans le but de mettre en place les alertes et dispositifs de prévention nécessaires (PRA/PCR). **C34.** Choisir et mettre en place des alimentations de secours en s'appuyant sur le dimensionnement des alimentations de secours afin d'assurer la continuité de fonctionnement des systèmes et réseaux informatiques.		**C33-C34 : Evaluation des points suivants :** • Des analyses proactives et réactives permettent d'identifier les causes d'incidents. Elles sont présentées et justifiées. • Les alertes et dispositifs deprévention sont en place. • La formation des utilisateurs à la détection des pannes est illustrée. • Les situations de handicap sont prises en compte dans le choix et l'adaptation des supports de diffusion par exemple. • Les principes de stabilité des alimentations sont connus et mis en œuvre. • Les alimentations de secours sont correctement dimensionnées. • La continuité est démontrée.

Compétence commune à tous les blocs de compétences :

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activitésexercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compristransversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
A25. Utilisation de l'anglais technique dans son activité professionnelle : - Compréhension d'une information technique à traduire ; - Veille technologique dans le secteur informatique.	**C35.** Maîtriser l'anglais technique dans son activité professionnelle afin de mener une veille efficace et comprendre une information technique relative à l'infrastructure systèmes et réseaux en anglais.	**Evaluation n°5 : Mise en situation professionnelle** - Production : Le candidat rédige un compte-rendu de veille technologique de son choix, relative à l'infrastructure systèmes et réseaux, documentée et étayée d'informations émanant de sites anglophones.	**C35 :** - Les sources de veille en anglais sont cohérentes et argumentées ; - Sa compréhension écrite de l'anglais est démontrée à travers la rédaction de son analyse des informations collectée.

Modalités d'évaluation

L'évaluation, reposant sur la participation effective à des opérations relevant de l'administration des réseaux et systèmes durant l'expérience en entreprise, est réalisée selon les trois modalités suivantes :

- Contrôle contenu : des évaluations ont lieu tout au long du dispositif de formation à travers des mises en situation professionnelle à partir de cas réels ou fictifs (rencontrées durant les périodes en entreprise, des cas pratiques, des QCM, des devoirs écrits, en phase avec les compétences du bloc. Les évaluations sont réalisées par l'équipe pédagogique ;

- Projet de fin d'étude composé de mises en situation professionnelle et soutenance orale devant un jury.

Modalités de validation de la certification professionnelle

La certification professionnelle Administrateur systèmes, réseaux et cybersécurité est composée de quatre blocs de compétences :

- **Modéliser une infrastructure systèmes, réseaux sécurisée et respectueuse de la politique RSE**
- **Déployer et administrer une infrastructure systèmes et réseaux sécurisée**
- **Assurer la maintenance d'une infrastructure systèmes et réseaux sécurisés**
- **Optimiser la performance des systèmes et réseaux informatiques sécurisés**

  - La validation partielle d'un bloc de compétences n'est pas possible.
  - Les blocs de compétences sont capitalisables.
  - L'évaluation de chaque bloc de compétences est réalisée via des modalités spécifiques d'évaluation détaillées dans le référentiel de la certification ci-dessus.
  - La réussite de(s) modalité(s) d'évaluation de ce bloc de compétences fait l'objet de la remise d'un parchemin de bloc de compétences.
  - La validation partielle de la certification est constituée des blocs dont la totalité des compétences est validée.