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 compris transversales, 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**
Concevoir et améliorer l'utilisation de l'infrastructure **A.1 Contribution à la définition de scénario de déploiement de l'infrastructure informatique**	C1.1 Recueillir les besoins relatifs à l'infrastructure en collaboration avec les équipes de la DSI et les utilisateurs afin d'évaluer les besoins en équipements, matériels, logiciels et services cloud ainsi que les niveaux de service requis auprès des fournisseurs.	**Modalité d'évaluation 1 : Mise en situation professionnelle reconstituée** Déroulement de l'épreuve : Les compétences de ce bloc sont évaluées sur la base d'une mise en pratique professionnelle permettant d'identifier si le candidat est capable de concevoir et améliorer une infrastructure technique en adéquation avec les besoins et les contraintes. Elle donne lieu à la rédaction individuelle d'un dossier de conception et d'amélioration et à la présentation orale individuelle de ce livrable devant un jury d'évaluation. **Durée** ‣ 4 jours pour la préparation de la mise en situation professionnelle reconstituée ‣ 30 minutes pour la présentation orale individuelle devant le jury, dont 10 minutes d'échanges.	**Pertinence du recueil de besoins :** - Les techniques de communication -écoute active, questionnement, reformulation- sont utilisées - Les besoins des utilisateurs et des autres parties prenantes (experts en cybersécurité, etc.) sont recensés en fonction des spécificités des métiers - Les matrices de choix sont correctement utilisées et complétées - Les choix prennent en compte la stratégie RSE de l'entreprise (économie d'énergie, frugalité numérique, etc.) - La prescription des matériels spécifiques aux personnes de situation de handicap est intégrée aux besoins et s'appuie sur les recommandations des acteurs en charge des situations de handicap - Les principes de base de l'organisation d'une entreprise et d'un prestataire de services informatiques (organigramme de l'entreprise / service informatique), et les liens fonctionnels entre services sont identifiés. - Les contraintes fonctionnelles et techniques de l'infrastructure sont pris en compte - L'ensemble des processus d'activité et des métiers de l'informatique sont identifiés - Le cycle de vie des services (phase de la stratégie des services, de la conception des services, de la transition des services, de l'exploitation des services et de l'amélioration continue des services) est identifié - Les fonctionnalités et les caractéristiques attendues (taille d'écran et autonomie pour un ordinateur portable, etc.) sont listées - Les indicateurs de suivi sélectionnés - disponibilité, fiabilité, temps de réponse, degré de satisfaction des utilisateurs, etc. - sont pertinents et en lien avec les processus de l'entreprise.

			- La conformité du niveau de service rendu et attendu est mesurée à partir d'indicateurs définis et relatifs aux plages d'ouverture du service, aux taux de suivi des incidents, aux taux de non-conformité, etc.
	C1.2 Proposer des scénarios d'évolution et d'amélioration de l'infrastructure cloud ou cloud hybride en y intégrant les aspects budgétaires et les contrats de services afin de conseiller la DSI ou les métiers sur les choix finaux.		**Qualité des propositions d'amélioration de l'infrastructure :** - Les éléments de performance d'une infrastructure (en particulier les flux) sont intégrés dans les scénarios proposés - Le schéma d'infrastructure proposé est complet et structuré en adéquation avec le recueil des besoins et les contraintes identifiées - Les spécificités d'une infrastructure cloud et cloud hybride (disponibilité des données, sécurité, coût, qualité, etc.) sont intégrées - Des solutions d'hébergement prenant en compte l'écoresponsabilité sont proposées (empreinte carbone de la donnée, etc.) - L'infrastructure existante est analysée et contient un descriptif des fonctionnalités, un schéma des flux, la liste des composants techniques, etc. - Les scénarios d'évolution et d'amélioration proposés sont fiables et complets : ils intègrent l'analyse de l'existant, la faisabilité économique, organisationnelle et technique du projet, des maquettes, un scénario de déploiement, une solution de sauvegarde, etc. - Les scénarios d'évolution et d'amélioration proposés sont argumentés : justification des choix techniques au regard du cahier des charges et du budget alloué, prise en compte de la pérennité de la solution proposée, etc.
	C1.3 Effectuer des choix d'implémentation détaillés (équipements, systèmes, réseaux) à partir du scénario validé, en s'appuyant sur les expertises des équipes internes et des prestataires afin de proposer une infrastructure optimisée et d'assurer la compatibilité des systèmes entre eux.		**Pertinence des choix d'implémentation :** - Le scénario de déploiement et le planning de déploiement sont définis - Les choix prennent en compte l'existant et ses contraintes (maintien en production, continuité de service, etc.) et sont compatibles avec les systèmes existants

			- Les tests de faisabilité sont menés et leurs résultats sont analysés et pris en compte
	C1.4 Mettre à jour la documentation, les procédures et consignes d'exploitation en s'appuyant sur les actions de maintien en condition opérationnelle (MCO) réalisées afin de décrire l'architecture du système d'information.		**Qualité de la mise à jour de la documentation, des procédures et des consignes :** - Les objectifs de la documentation, des procédures et des consignes d'exploitation sont formulés - La documentation d'architecture technique du SI est mise à jour - Les procédures et consignes d'exploitation (documents d'installation, procédures de mise à jour, consignes d'exploitation, etc.) sont mises à jour - Le vocabulaire technique est adapté lors de l'écriture des différents documents
A.2 Mise en place d'une infrastructure sécurisée	C1.5 Participer à l'évaluation des risques de cybersécurité avec l'appui des experts et des outils mis à disposition par l'ANSSI et les constructeurs/éditeurs afin de contrôler le niveau de sécurité des systèmes et de repérer les failles de sécurité potentielles.		**Qualité de la participation dans l'évaluation des risques :** - Les risques liés à la sécurité des systèmes et réseaux (fuite de données, attaque, etc.) sont identifés - Les rôles des parties prenantes dans l'évaluation des risques de cybersécurité (experts Sécurité des Systèmes d'Information et Security Operation Center) sont identifiés - Les principaux documents (de la politique de sécurité et d'analyse des risques, etc.) sont identifiés et des mises à jour sont proposées - L'analyse des risques est comprise - Les outils de l'ANSSI (guides, référentiels, etc.) sont connus et utilisés à bon escient - Les ressources produites par les constructeurs et les éditeurs de logiciels (méthodologie, bonnes pratiques, etc.) sont connues et utilisées à bon escient - Les alertes sont remontées en cas d'incident, dans le respect des procédures en vigueur dans l'entreprise, aux bons interlocuteurs, et en adaptant sa posture et sa communication aux personnes et notamment aux personnes en situation de handicap, etc.

	C1.6 Prendre en compte les mesures nécessaires au respect de la protection des données personnelles et de l'accessibilité numérique afin de respecter la réglementation en vigueur.		**Qualité du respect de la règlementation en vigueur :** - Les règlementations en vigueur (RGPD, RGAA, etc.) sont respectées - Les mesures et les pratiques en matière de protection des données et d'accessibilité numérique (Guide de l'hygiène informatique de l'ANSSI, etc.) sont identifiés et appliquées - La charte informatique est identifiée et respectée - Les alertes sont remontées en cas de non-respect de la charte informatique et de la règlementation (respect des procédures en vigueur dans l'entreprise, alerte aux bons interlocuteurs, etc.)
	C1.7 Collaborer avec des équipes internes et des prestataires en utilisant des techniques et des méthodes de gestion de projet afin de réaliser l'infrastructure avec les parties prenantes.		**Qualité de la collaboration :** - Les principales méthodes de gestion de projet (classiques, agile, etc.) sont utilisées tout au long des cycles de vie d'un projet sont connus - Les échanges avec les différentes parties prenantes sont adaptés en fonction du rôle et des missions de chacune : chefs de projet, SOC, comités de pilotage, prestataires, etc. - L'administrateur systèmes et réseaux identifie sa place et son rôle au sein d'une équipe projet - Les principales techniques de communication sont utilisées lors des interventions au sein du projet (écoute active, questionnement, reformulation, etc.)
A.3 Mise en œuvre d'une veille dans le domaine du numérique	C1.8 Identifier les tendances technologiques et réglementaires en mettant en place des outils de veille afin de garantir l'optimisation des systèmes de l'entreprise avec les dernières évolutions.		**Qualité de la veille :** - Les outils et ressources de veille technologique et règlementaires (moteurs de recherche, agrégateurs de flux, agrégateurs d'actualité, blogs, etc.) sont déterminés et utilisés - La fiabilité et la valeur des informations recueillies est vérifiée - Le vocabulaire technique (français / anglais) est utilisé

	C1.9 Diffuser une veille technologique et réglementaire en définissant le système de veille afin d'améliorer en continue les systèmes de l'entreprise		**Qualité de la diffusion de la veille :** - Les modalités de diffusion et de partage de la veille sont définis et adaptés aux publics visés - Les évolutions technologiques et leurs impacts sur l'infrastructure de l'entreprise sont analysés

Tester et mettre en production les ressources et assurer leur amélioration continue
 	
A.4 Déploiement de la solution informatique
	C2.1 Formaliser un plan de tests en déclinant les phases d'analyse afin que la solution mise en place réponde aux exigences fonctionnelles et de sécurité.	**Modalité d'évaluation 2 : Mise en situation professionnelle reconstituée**
		
		Déroulement de l'épreuve :
		
		Les compétences de ce bloc sont évaluées sur la base d'une mise en pratique professionnelle permettant d'identifier si le candidat est capable de mettre en œuvre l'infrastructure tout en assurant son amélioration.
		
		Elle donne lieu à la rédaction individuelle d'un dossier d'intégration et à la présentation orale individuelle de ce livrable devant un jury d'évaluation.
		
		Durée
		- 4 jours pour la préparation de la mise en situation professionnelle reconstituée
		- 30 minutes pour la présentation orale individuelle devant le jury, dont 10 minutes d'échanges
			Pertinence du plan de test :
			- L'existant est vérifié :
			  - Les éléments de l'infrastructure existante (systèmes, stockage et réseaux) sont installés et configurés ;
			  - L'infrastructure d'interconnexion (commutateur, routeur, etc.) est vérifiée ;
			  - Les services associés (authentification, habilitation, protocole DHCP, etc.) sont installés et paramétrés ;
			  - Les travaux annexes préalables (câblage, électricité, etc.) sont vérifiés ;
			  - Les logiciels de sécurité (antivirus, chiffrement des données et d'accès tels que pare-feu, anti-intrusion, proxy, etc.) sont installés et configurés ;
			  - Les accès aux services (accès distants, FTP, VPN, etc.) sont paramétrés et contrôlés.
			- Les objectifs du plan de test vérifient la conformité de la solution aux besoins des parties prenantes (utilisateurs finaux, DSI, cybersécurité) et la sécurité
			- Le plan de test comprend toutes les étapes (phase pilote avec les experts logiciels et matériels, phase de pré-production avec une population ciblée d'utilisateurs, phase de production pour le déploiement global dans l'ensemble de l'entreprise, traitement des anomalies, etc.) et anticipe les problèmes (analyse, modélisation, scénarios de tests)
			- Les principaux outils d'automatisation et de supervision (Nagios, Zabix, etc.) sont identifiés
			- Un plan de retour arrière comprenant tous les cas de figure envisageables est défini

	C2.2 Réaliser les mises en production des solutions informatiques à l'aide de la documentation d'exploitation, des outils d'automatisation et des outils de supervision afin de s'assurer de la répétabilité des actions et de la robustesse du SI.		**Qualité des mises en production de nouvelles ressources :** - La documentation d'exploitation de l'existant (procédures, architecture, etc.) est identifiée et respectée - Les prérequis (dernière sauvegarde avant arrêt, information aux utilisateurs, etc.) sont vérifiés et pris en compte - Les méthodes, procédures et processus standardisés pour gérer les changements sont intégrés et respectés - Les scripts d'automatisation (programmation en python, en shellscript, en powershell, etc.) et de lancement de traitement différés sont écrits et testés - Les mises en production des solutions choisies sont réalisées dans le respect du scénario prédéfini - Le fonctionnement des nouvelles solutions intégrées est vérifié - Les procédures d'installation et de configuration d'environnement de travail sont automatisés (utilisation d'outils adaptés et performants) dans le respect du cadrage du projet
	C2.3 Assurer les mises à jour mineures / majeures et les montées de version en appliquant les bonnes pratiques du fournisseur ainsi que les règles définies par la direction informatique et/ou la direction de la sécurité afin de garantir l'intégrité du SI et de maintenir sa performance.		**Pertinence des actions de mise à jour et des montées de version :** - Un planning des opérations de maintenance est élaboré (en fonction de leur criticité, impact sur l'ouverture du service, etc.) - Les préconisations des experts (fournisseur éditeur ou constructeur) et les règles définies par la direction informatique et/ou la direction de la sécurité sont connues et prises en compte - L'inventaire des configurations matérielles et logicielles du parc d'équipement actif est ajusté / tenu à jour - Les changements effectués sont tracés dans la documentation d'exploitation
A.5 Support de la solution informatique	C2.4 Assurer le support aux utilisateurs et éventuellement aux équipes techniques lors de la mise en production en recueillant les dysfonctionnements repérés afin de résoudre les problèmes techniques.		**Qualité du support aux utilisateurs et aux équipes techniques :** - Les techniques de communication sont connues et appliquées avec les utilisateurs et les équipes techniques (consignes et explications factuelles, vocabulaire adapté, pédagogie, etc.)

			- Les actions d'information proposées sont pertinentes (actions d'information, mise à disposition d'outils et de documentations, FAQ, transfert de compétences, etc.) et adaptées au public visé - Le moyen de communication est adapté en fonction des situations de handicap rencontré (mobilisation des ressources disponibles, appui d'un référent handicap, etc.) - Un retour arrière sur la mise en production effectuée est proposé le cas échéant - La communication autour du respect des règles d'utilisation définies est pertinente (actions de sensibilisation, pédagogie autour des règles, respect de la charte le cas échéant, etc.)
	C2.5 Mettre à jour les référentiels de production en s'appuyant sur des logiciels d'analyse et d'extraction afin de générer des rapports répondant aux besoins de la DSI.		**Pertinence du suivi des actions menées :** - Les outils permettant de décrire les différents actifs du SI (CMDB, etc.) sont utilisés - La documentation d'exploitation (schémas d'infrastructure physique et logique, procédures d'exploitation et de configuration, etc.) et les référentiels de production (analyse des infrastructures existantes, niveau de licence, qui à quel logiciel, etc.) sont rédigés selon les règles de l'art (exhaustivité, orthographe, grammaire, etc.) et mis à jour - Les modes opératoires sont rédigés ou mis à jour - Les rapports générés répondent aux besoins de la DSI. - L'accès aux documents clés est facilité par l'utilisation d'un plan de classement adéquat

Administrer l'infrastructure et la maintenir en activité **A.6 Contrôle des éléments de sécurité et configuration des outils de supervision**	C3.1 Définir la configuration des composants de sécurité, des comptes utilisateurs et des postes de travail en appliquant les politiques de sécurité définies par l'entreprise afin de sécuriser l'environnement utilisateur (poste de travail, terminaux mobiles, etc.).	**Modalité d'évaluation 3 : Mise en situation professionnelle reconstituée** Déroulement de l'épreuve : Les compétences du bloc n°3 sont évaluées sur la base d'une mise en pratique professionnelle permettant d'identifier si le candidat est capable de superviser, sécuriser et gérer une infrastructure en proposant une maquette. Elle donne lieu à la rédaction individuelle d'un dossier d'administration et à la présentation orale individuelle de ce livrable devant un jury d'évaluation. **Durée** › 4 jours pour la préparation de la mise en situation professionnelle reconstituée › 30 minutes pour la présentation orale individuelle devant le jury, dont 10 minutes d'échanges	**Pertinence de la configuration des droits d'accès :** - L'outil de suivi et d'analyse des droits d'accès (habilitations) utilisé répond aux règles de sécurité définies (intégrité, disponibilité, accessibilité, confidentialité, traçabilité et restriction de diffusion des informations) - La conformité des droits d'accès est justifiée à partir d'une revue des habilitations - Les paramètres de la revue des habilitations sont définis (acteurs à impliquer, revue périodique ou continue, fréquence, temps nécessaire, délais impartis, éventuels freins, etc.) en fonction des objectifs visés (type d'événement : départ de l'entreprise, congé maternité, arrêt de travail, changement de poste, etc.)
	C3.2 Administrer les autorisations d'accès pour les utilisateurs en effectuant un suivi régulier afin de prévenir et de réduire les risques de malveillance internes ou externes.		**Pertinence de l'administration des autorisations d'accès :** - Les comptes utilisateurs et/ou les postes de travail sont créés, modifiés, supprimés dans le respect des consignes (RH, direction, etc.) - Un audit de gestion du compte utilisateur et/ou du poste de travail est effectué dans le respect des règles de l'entreprise - Un rapport est généré et transmis au requérant (RH, direction, DSI, expert, etc.) - Les points de défaillance potentiels (sécurisation des protocoles utilisés, utilisation d'outils de surveillance, analyse des journaux systèmes, utilisation d'antivirus, gestion des habilitations, etc.) sont identifiés et vérifiés
	C3.3 Réaliser le suivi des systèmes (contrôle des systèmes de sauvegarde, d'antivirus, des éléments de sécurité, etc.) en s'aidant des outils de supervision afin de les maintenir en condition opérationnelle.		**Qualité du suivi des systèmes :** - Le plan de maintien en condition opérationnelle est fiable - Les sauvegardes (Veeam, Avamar, etc.) sont testées - Les politiques et définitions d'antivirus (Microsoft, Mac Afee, etc.) sont à jour

			- Les mises à jour logicielles sont appliquées, vérifiées et validées
	C3.4 Assurer la supervision technique de l'infrastructure (matériels, réseaux, serveurs) en utilisant les outils de supervision mis en place afin de détecter et de traiter au plus tôt les incidents globaux.		**Qualité de la supervision technique :** - Les outils de supervision (Centreon, etc.) sont connus et utilisés - Les éléments à superviser (processeur, mémoire, stockage, commutateurs, débits, contrôle des flux, etc.) sont identifiés - Des indicateurs et des seuils de performance et/ou de criticité sont définis et justifiés - Le choix des alertes est pertinent (canal, périodicité, etc.) - La procédure de vérification et de traitement est adaptée (tests de la solution de supervision) - Les incidents globaux sont contournés, résolus ou escaladés le cas échéant
A.7 Résolution d'un incident et support aux utilisateurs	C3.5 Assister les utilisateurs dans la résolution de leurs demandes en apportant des réponses adaptées afin de garantir leur satisfaction.		**Qualité de la gestion des demandes :** - L'outil de gestion des demandes est maîtrisé et utilisé correctement - Les demandes (matériel, équipement, etc.) sont méthodiquement analysées et prises en charge - Les techniques de communication sont connues et mobilisées correctement avec les utilisateurs et les équipes techniques (consignes et explications claires, vocabulaire adapté, bienveillance, etc.) - Les réponses apportées sont argumentées et justifiées - Les utilisateurs sont accompagnés dans la prise en main des nouveaux matériels - Les bonnes pratiques en matière de Green IT (économie d'énergie, privilégier les matériels recyclés, etc.) sont connues et prises en compte - L'environnement de travail de l'utilisateur (situation de handicap, etc.) est pris en compte
	C3.6 Gérer un incident informatique en conduisant une analyse des causes afin d'apporter un correctif ou un		**Qualité de la gestion des incidents :** - L'outil de gestion des incidents est utilisé

	contournement et d'informer les parties prenantes.		- Les demandes, alertes et messages sont analysés, classés et priorisés en fonction du niveau de criticité des risques - Les incidents sont identifiés, analysés et tracés - La méthodologie proposée pour résoudre l'incident est pertinente (impact minimal sur la production, etc.) - Les incidents et/ou problèmes (matériels, logiciels et réseaux) sont corrigés (à l'appui des connaissances, des notices constructeurs, des guides d'exploitation, des aides en ligne, des sites Web, des supports techniques, etc.) - La procédure d'escalade vers le service ou interlocuteur concerné est mise en place le cas échéant (prise de contact avec l'éditeur ou le constructeur, passage de relais à un expert, etc.) - Les parties prenantes (utilisateurs, équipes IT, etc.) sont informées de la solution apportée.