RECRUTEMENT DE CONSULTANTS POUR LA FORMATION DU PERSONNEL DE LA FONCTION IT DE LA BOAD

2025 - 2027

APPEL D'OFFRE

Sept. 2025
https://www.boad.org

SOMMAIRE

CONTEXTE DU PROJET

Créée en 1973 et opérationnelle depuis 1976, la Banque Ouest Africaine de Développement (BOAD) est une institution commune de financement du développement des États de l'Union Économique et Monétaire Ouest Africaine (UEMOA). Elle est un établissement public à caractère international qui a pour objectif de promouvoir le développement et l'équilibre des États membres et de réaliser son intégration économique en finançant des projets prioritaires de développement.

Pour renforcer l'impact de ses interventions en termes de résultat de développement de ses États membres, la BOAD s'est dotée d'un plan stratégique appelé Plan DJOLIBA sur la période 2021-2025. La mise en œuvre de ce plan stratégique implique des changements majeurs en termes de modernisation, de sécurisation du SI et de digitalisation des processus.

C'est dans ce contexte, que la BOAD a initié l'élaboration et la mise en œuvre d'un Schéma Directeur du Système d'information (SDSI) 2021-2025. Ce programme SDSI, appelé SIRBA, couvre un portefeuille de cinquante (50) projets regroupés en cinq (5) chantiers et subdivisés en huit (8) comités techniques.

Au vu de toutes les innovations technologiques envisagées dans son système d'information, la BOAD a prévu dans le cadre du SDSI d'investir sur son personnel en renforçant les compétences de l'équipe IT à travers la mise en œuvre d'un plan de formation afin de se doter des compétences internes sur les sujets tels que le Cloud, Cyber, Architecture d'entreprise, Data Analytics.

Ainsi, la **BOAD** à la suite d'un appel d'offre a confié à **SMARTIC** la mission d'élaborer un plan de formation triennal pour son personnel IT et de veiller au recrutement de prestataires qualifiés, aptes à assurer la mise en œuvre effective des formations qui en découlent. C'est dans ce cadre que le présent appel d'offre est lancé.

Titre I : CLAUSES ADMINISTRATIVES

Article 1 : Objet de l'appel d'offres

Le présent appel d'offres a pour objet : **LA REALISATION DU PLAN DE FORMATION TRIENNAL 2025-2027 DU PERSONNEL IT de la BOAD.**

Article 2 : Conditions d'éligibilité

Le présent appel d'offres est ouvert à toute personne morale et groupement d'entreprises ayant les capacités juridiques, techniques et financières nécessaires à l'exécution du présent marché. Tout(e) candidat(e) doit en outre, justifier de capacités juridiques, techniques, administratives et financières nécessaires pour l'exécution des prestations décrites au titre II (clauses techniques et particulières) du présent cahier des charges.

Article 3 : Connaissances des lieux, conditions de travail ou de fournitures de prestation

Par le fait d'avoir fait acte de candidature, le (la) soumissionnaire reconnaît notamment :

S'être assuré(e) :

- De la nature et des conditions de réalisation du marché ;
- Des problèmes à résoudre pour la bonne exécution du marché ;
- De toutes les conditions et circonstances susceptibles d'avoir une influence sur l'exécution du marché ou sur les prix;
- Avoir établi sous son entière responsabilité les coûts pour chaque service ou prestation, lesquels ne pourront en aucun cas être remis en cause, ni faire l'objet de modification ou réclamation de quelque nature que ce soit.

Toute carence, erreur ou omission de l'adjudicataire du marché quant à la connaissance de la nature et des conditions de travail ou de fourniture de service ou prestation engagent sa seule responsabilité.

Article 4 : Dépôt, présentation des offres et pièces à fournir

4 -1 : Dépôt du dossier

Les soumissions doivent être envoyées au plus tard le **17 Octobre 2025 à 17 heures 00 minute** en version électronique sécurisée par un mot de passe à l'adresse suivante : consultformationit@boad.org avec pour intitulé « SOUMISSION PLAN DE FORMATION BOAD 2025-2027 ». Le(s) lots, le(s) modules ainsi que leurs numéros correspondants devront être précisés dans le corps du mail.

Le nom du soumissionnaire ainsi que le mot de passe devront être envoyés à l'adresse suivante : leon.boni@smartic.ci

NB : Aucune offre ne sera recevable au-delà du délai indiqué plus haut.

4 - 2 : Présentation du dossier

IMPORTANT : les documents composant la soumission à l'appel d'offres devront comprendre obligatoirement les pièces administratives, une offre technique et une offre financière.

Ils devront obligatoirement être dans des fichiers numériques différents portant le nom du soumissionnaire et les mentions :

« Pièces Administratives »

« Offre technique » ;

« Offre financière ».

Les documents transmis devront être réalisés aux formats usuels de rédaction documentaire. Les formats acceptés sont (*.pdf, *.docx). Les fichiers compressés mis à disposition devront également être réalisés aux formats usuels. Les formats acceptés sont (*.zip, *.rar).

Le fichier compressé (*.zip ou *.rar) doit être obligatoirement sécurisé par un mot de passe au choix du soumissionnaire.

NB : le dossier d'appel d'offres est rédigé avec la police (Century Gothic) en taille 13 pour les titres et la taille 12 pour le corps du document.

4 - 3 : Composition des pièces administratives à fournir

Les soumissions devront comprendre :

- La déclaration fiscale d'existence (DFE)

- La lettre de soumission à l'appel d'offres (voir le modèle en annexe) ;
- Le capital social de l'entreprise ;
- Le chiffre d'affaires du dernier exercice clos ;
- L'attestation d'inscription au registre de commerce ;
- Les références bancaires ;
- La localisation précise du siège social de l'entreprise (plan de localisation) ;
- Les références techniques (attestations de bonne exécution) ;
- Autorisation d'installation ou la carte d'opérateur économique en cours de validité ;
- Certificat d'inscription au Registre de Commerce et du Crédit Mobilier (RCCM) ;
- Attestation en cours de validité certifiant que le soumissionnaire est en règle vis-à-vis de l'administration fiscale ;
- Attestation en cours de validité certifiant que le soumissionnaire est en règle vis-à-vis de la Sécurité Sociale ;
- Curriculum vitae des principaux dirigeants ;
- Assurance responsabilité Civile de l'entreprise ;
- Attestation de non-faillite datant de moins de trois (03) mois.

Article 5 : Additifs au dossier d'appel d'offres, éclaircissements

La BOAD se réserve le droit de demander des documents complémentaires au cours de l'analyse des offres. Le cas échéant, ces demandes seront transmises aux soumissionnaires concernés.

Article 6 : Garantie

Le/la soumissionnaire doit proposer une durée particulière de garantie des offres. Cette condition, pour être prise en compte

dans l'évaluation de l'offre, devra être écrite de manière expresse.

Article 7 : Frais engagés par le soumissionnaire

Le soumissionnaire supporte tous les frais liés à la préparation et au dépôt de sa candidature. La BOAD n'est en aucun cas responsable de ces frais, ni tenue de les rembourser, quel que soit le déroulement ou l'issue de la procédure d'appel d'offres.

Article 8 : Délai de validité des offres

Le soumissionnaire restera lié par son offre pour une durée de 120 jours calendaires, à compter de la date limite de dépôt des offres indiquée à l'article 4.1 du présent cahier des charges.

Article 9 : Délai de livraison ou d'exécution

Pour le présent marché, le délai de livraison ou d'exécution devra être précisé par le soumissionnaire.

Article 10 : Considérations budgétaires

Pour des raisons de limitation budgétaire, la BOAD pourrait négocier avec le fournisseur la possibilité d'ajuster les coûts du marché en reconsidérant l'offre financière du soumissionnaire.

Article 11 : Respect des conditions d'appel d'offres

Toute offre qui ne respectera pas les présentes conditions d'appel d'offres ou qui contiendra des réserves de quelque nature que ce soit, sera déclarée nulle et non avenue. L'offre doit être envoyé conformément aux dispositions de l'article 4 du présent cahier de charge.

Article 12 : Modification - retrait

Le soumissionnaire peut modifier ou retirer son offre après sa soumission, à condition que la notification écrite de la modification ou du retrait soit reçue sept (7) jours avant la date de clôture des soumissions.

La notification de modification ou de retrait de l'offre par le soumissionnaire sera envoyée par courriel à l'adresse consultformationit@boad.org . Elle devra en outre porter la mention « modification » ou « retrait » selon le cas.

Aucune offre ne peut être modifiée ou retirée après la date limite d'envoi des offres.

Article 13 : Vérification, critères d'évaluation et appréciation des conditions du marché

13 -1 : Vérification des offres

L'examen des dossiers portera sur la vérification des pièces administratives, techniques et financières reçues.

La Commission d'analyse des offres se réserve, par ailleurs, le droit de convoquer un soumissionnaire, aux frais de ce dernier, pour lui demander des explications complémentaires nécessaires à l'examen de l'offre ou concernant les omissions ou erreurs relevées dans celle-ci.

Le soumissionnaire dont l'offre n'est pas retenue, ne peut contester pour quelque motif que ce soit.

13 - 2 : Critères d'évaluation

Les offres sont appréciées notamment, sur la base des critères d'évaluation administratifs, techniques et financiers prédéfinis au titre II (clauses techniques et particulières).

13 -3 : Appréciation des conditions du marché

La BOAD peut décider d'organiser une visite des locaux d'un ou des soumissionnaire(s) afin d'apprécier l'environnement, les installations ou les équipements destinés à assurer l'exécution du marché.

Article 14 : Critère d'attribution de marché

Sous réserve des dispositions de l'article 13, la BOAD attribuera le(s)marché(s) au(x) soumissionnaire(s) le(s) mieux disant(e)s.

L'adjudicataire recevra une notification à son adresse de l'attribution du marché à laquelle sera joint un projet de contrat de prestation de services.

Article 15 : Droit d'annulation de la procédure d'appel d'offres

Nonobstant les dispositions de l'article 11, la BOAD se réserve le droit d'annuler la procédure d'appel d'offres à tout moment avant l'attribution du marché, sans de ce fait, encourir une responsabilité quelconque vis-à-vis du ou des soumissionnaire(s).

Titre II : CLAUSES TECHNIQUES ET PARTICULIERE

1- Objectifs

1-1 : Objectif général

L'objectif de cette consultation est de procéder au recueillement des offres techniques de formations à la lumière des besoins exprimés dans le présent cahier de charge.

1-2 : Objectifs spécifiques

Plus spécifiquement, le présent appel d'offre consiste à atteindre les objectifs suivants :

- Recueillir les offres techniques de formation à même de permettre l'acquisition des compétences indiquées dans ce présent cahier de charges
- Recueillir les offres financières soutenant chaque offre technique ;
- Sélectionner les prestataires présentant les meilleures offres sur la base des critères de sélection ;
- Elaborer le plan de formation budgétisé ;
- Elaborer le calendrier d'exécution des actions de formation.

2- Résultats attendus

- Les exigences relatives aux objectifs de compétences mentionnés dans le présent cahier des charges sont connues et validées par le prestataire sélectionné ;
- L'investissement nécessaire pour chaque formation est connu ;
- Les prestataires présentant les meilleures offres sont sélectionnés ;
- Le plan de formation budgétisé est élaboré ;
- Le calendrier d'exécution des actions de formation est élaboré.

3- Population à former

Le programme général de formation couvre l'ensemble du personnel de la fonction IT de la BOAD. Pour chaque thème, la population cible est indiquée. Les formations énoncées dans ce cahier des charges seront réparties sur les trois (03) années.

4- Programme de base

Les organismes de formation doivent proposer un programme de base qui sera adapté aux réalités et besoins de la fonction IT de la BOAD.

5- Durée

Les formations doivent se dérouler sur une durée acceptable permettant aux formateurs de transmettre de façon suffisante les savoirs et savoir-faire. Dans tous les cas, la durée devrait se situer entre deux jours et cinq jours avec un maximum de dix jours.

6- Volume horaire

Le volume horaire total de chaque session de formation doit être au moins égale à quatorze heures, tout en respectant les conditions d'efficacité.

7- Méthodes pédagogiques

Les méthodes pédagogiques doivent être précisées. Celles ayant un caractère pratique sont recommandées.

L'utilisation de plusieurs méthodes pendant la même formation est souhaitée (cours magistral, travaux pratiques, échanges, simulations, exercices d'application, vidéos etc.).

Pour chaque formation, il doit être remis à chaque participant ainsi qu'au Capital Humain de la BOAD, un support de cours au choix : support papier, CD, clé USB, documents électroniques (par mail) etc. au plus tard à la fin de la formation.

8- Evaluation de la formation

A l'effet d'évaluer les acquis de la formation, le formateur procèdera en début de formation à une évaluation d'entrée et à une évaluation de sortie à la fin de la formation. Les scores issus de ces deux évaluations devront être transmis à la BOAD dans le rapport de fin de formation

Le formateur procédera également à la mesure de la satisfaction des auditeurs à la fin de la formation, par le biais du support élaboré à cet effet par la BOAD.

9- Condition de réalisation de la formation et de la restauration

Les formations devront se dérouler dans des conditions qui garantissent leur efficacité. Chaque organisme de formation participant à l'appel d'offres est tenu d'indiquer dans son dossier ses moyens matériels et didactiques pouvant contribuer à la réussite des actions de formation. Il s'agit notamment des :

- Salles de formations
- Moyens didactiques : TV, camera, vidéo projecteurs, matériels informatiques etc., selon le type de formation ;
- Supports de cours et autres documents ;
- Pauses café et déjeuners servis, devront respecter les normes d'hygiène.

10- Conditions relatives aux thèmes de formation

Pour chaque thème de formation retenu par le prestataire, il doit être produit un document comportant :

- L'intitulé de la formation ;
- La présentation de la formation ;
- Les objectifs pédagogues ;
- Les résultats attendus ;
- Les prérequis au cas échéant ;
- La population cible ;
- Le syllabus de la formation ;
- Les moyens et méthodes andragogiques ;
- Les modalités d'évaluation des acquis ;
- Les outils didactiques ;
- La durée en volume horaire et en jour de la formation ;
- Les qualifications, certifications et références du formateur par thème choisi ;
- Les références de l'organisme de formation ou son expérience dans le domaine de la formation continue notamment en ce qui concerne le thème choisi ;
- Le coût total ;
- Indiquer le lieu de la formation si en présentiel ;

11- Dispositions relatives à la fin de la formation

A la fin de la formation, le prestataire devra produire un rapport de fin de formation portant sur les aspects suivants :

- La ponctualité et l'assiduité des participants ; la motivation et le sérieux des participants ;
- L'évaluation de la formation : le niveau de satisfaction des participants au plan technique (contenu du programme, animation de la formation, compétences du formateur, applicabilité des connaissances, supports de cours et documentation, accueil et commodités pendant la formation) ;
- Les observations et souhaits des participants ;
- L'appréciation globale du formateur : niveau de connaissances des participants avant et après la formation, réactivité des participants, motivation, etc.

Il doit aussi :

- Fournir à la BOAD, une copie du support du cours sous format papier ou électronique ;
- Remettre à chaque participant un support de cours et une attestation de formation.

12- Profil des formateurs

Chaque formation doit être réalisée par des consultants à la fois spécialistes et professionnels de la discipline ou de leurs domaines. L'organisme de formation doit donc indiquer l'identité et les références des formateurs proposés pour chaque action de formation, en prenant soin de joindre les Curriculums Vitae et les certifications.

13- Coût de la formation

Pour chaque action de formation, le prestataire devra indiquer le coût hors taxe et TIC ainsi que le coût par participant en tenant compte des prix du marché.

Le prix proposé pour chaque action de formation peut être révisé avec les organismes retenus.

14- Liste des champs de formation

- LOT 1 : FORMATIONS TRANSVERSALES
- LOT 2 : FORMATIONS ADMINISTRATIVES
- LOT 3 : FORMATIONS MANAGERIALES
- LOT 4 : FORMATIONS TECHNIQUES

LISTE DES DOMAINES DE FORMATION PAR LOT

LOT 1 : FORMATIONS TRANSVERSALES

N°	THEME DE FORMATION	OBJECTIFS DE COMPETENCES	PUBLIC CIBLE	EFFECTIF	FORMATEUR
01	**FORMATION SOFT SKILLS – GESTION DE L'IMPREVU, PRISE DE DECISION RAPIDE**	• S'approprier une méthode de gestion du • Temps et de planification des activités ; • Découvrir les règles de la gestion des • Priorités et savoir identifier et prioriser • Ses actions selon les aléas ; • Gérer les annulations, reports et • Imprévus externes ; • Prendre du recul pour traiter les • Situations rationnellement et dans les délais • Rebondir efficacement	Chargé du pilotage SI (PMO)	01	✓ Formation supérieure de niveau Bac+5/6 au minimum en Management, RH ; ✓ Au moins dix (10) années dans l'enseignement et /ou la formation continue ; ✓ Expérience avérée dans l'animation du thème de formation.
02	**Méthodes de résolution de problèmes – 8D, Ishikawa, QQOQCCP**	• Caractériser un problème, • Comprendre la démarche 8D, • Connaître les étapes et outils associés (QQOQCCP, brainstorming, Ishikawa/5 M, vote pondéré, 5 Pourquoi) • Aborder les problèmes de manière structurée, • Animer la résolution de problèmes, • Utiliser les outils • Adopter un rôle d'animateur responsabilisant les collaborateurs	Responsable de la Sécurité du Système d'information	01	✓ Formation supérieure de niveau Bac+5/6 au minimum en Management, RH ; ✓ Au moins dix (10) années dans l'enseignement et /ou la formation continue ✓ Expérience avérée dans l'animation du thème de formation
03	**FORMATION DES FORMATEURS – INITIATION A L'ANDRAGOGIE**	• Construire un programme pédagogique clair. • Définir les objectifs pédagogiques ; • Conduire efficacement une session (captiver l'attention, utiliser les supports adaptés) • Animer avec assurance et aisance des actions de formation destinées à des adultes en activité professionnelle ; • Favoriser l'implication des apprenants adultes. • Rendre une formation captivante et gérer la diversité des profils. • S'assurer de la qualité de sa formation • Évaluer les acquis d'une formation	Responsable des Infrastructures, Réseaux et Support	01	✓ Formation supérieure de niveau Bac+5/6 au minimum en management des RH ; ✓ Au moins dix (10) années dans la formation des formateurs ✓ Expérience avérée dans l'animation du thème de formation
04	**COLLABORER EFFICACEMENT AVEC SON MANAGER**	• Comprendre les enjeux de la collaboration entre assistante et manager • Faciliter le relationnel avec son manager • Développer des outils efficaces pour appuyer les décisions de son manager • Renforcer la relation avec son manager pour plus d'efficacité et de sérénité • Maîtriser sa communication verbale et non-verbale • Identifier et comprendre le style de personnalité de son manager • Prendre la parole efficacement en réunion • Argumenter pour faire passer ses idées • Faire face aux situations difficiles avec assertivité	Secrétaire Responsable confirmée I	01	✓ Formation supérieure de niveau Bac+5/6 au minimum en Management, RH ; ✓ Au moins dix (10) années dans l'enseignement et /ou la formation continue ✓ Expérience avérée dans l'animation du thème de formation

05	**TECHNIQUE D'EXPRESSION ORALE**	• Comprendre l'importance d'une bonne expression dans le cadre professionnel • Mobiliser et classer ses idées • Gagner en aisance à l'oral (comme à l'écrit) pour les interventions professionnelles	Secrétaire Responsable confirmée I	01	✓ Formation supérieure de niveau Bac+5/6 au minimum en management des RH ; ✓ Au moins dix (10) années dans la formation des formateurs ✓ Expérience avérée dans l'animation du thème de formation
06	**COMMUNICATION ET GESTION DU STRESS UTILISATEUR**	• Comprendre les mécanismes du stress Se connaître et identifier ses sources de stress • Développer adaptabilité et résistance au stress • Gérer ses émotions et construire une méthode personnelle pour une efficacité accrue	Technicien maintenance et support Confirmé II Secrétaire Responsable confirmée I	02	✓ Formation supérieure de niveau Bac+5/6 au minimum en Management, RH, Psychologie ; ✓ Au moins dix (10) années dans l'Enseignement et /ou la Formation Continue. ✓ Expérience avérée dans l'animation du thème de formation

LOT 2 : FORMATIONS ADMINISTRATIVES

N°	THEME DE FORMATION	OBJECTIFS DE COMPETENCES	PUBLIC CIBLE	EFFECTIF	FORMATEUR
01	**METHODOLOGIES ITIL POUR LE SUPPORT ET LA GESTION DES INCIDENT**	• Évaluer la maturité et les capacités de la pratique de gestion des incidents ITIL • Appliquer les concepts clés, processus, rôles et compétences spécifiques à la gestion des incidents • Comprendre comment l'information, la technologie, partenaires et fournisseurs soutiennent cette pratique	Technicien maintenance et support Confirmé II	01	✓ Certifications recommandées **: ITIL® 4 Foundation,** ITIL® 4 Managing Professional (Atout) ✓ Avoir déjà formé des équipes IT opérationnelles (support, gestionnaires d'incidents, superviseurs) ✓ Savoir connecter les processus ITIL aux réalités quotidiennes des équipes
02	**ORGANISATION ET GESTION DE PROJETS SI POUR NON-INFORMATICIENS**	• Comprendre les fondamentaux des systèmes d'information (SI) • Identifier les étapes clés d'un projet SI • Contribuer efficacement au pilotage d'un projet SI • Collaborer avec les acteurs techniques et les métiers • Utiliser les outils et méthodes de gestion de projet • Identifier les risques, enjeux et facteurs clés de succès d'un projet SI	Secrétaire Responsable confirmée I	01	✓ Certifications recommandées : **CAPM/PMP/Prince2/PM²/AgilePM, ITIL4 Foundation** ✓ Connaissance pratique des méthodes classiques (cycle en V, PMP) et agiles (Scrum, Kanban, hybride) ✓ Avoir animé des projets de transformation numérique ou applicative avec des équipes métier ✓ Avoir l'habitude de travailler avec des non-techniciens ✓ Être capable de structurer un projet, d'expliquer sans jargon, et d'impliquer les acteurs

03	**GESTION DOCUMENTAIRE ET NUMERIQUE COLLABORATIVE**	• Mettre en place un espace documentaire collaboratif (sur SharePoint/Teams), organiser les contenus selon plan de classement, droits d'accès, métadonnées • Gérer les documents internes du cycle de vie à l'archivage, produire un tableau de gestion documentaire • Capitaliser les connaissances : animer des groupes de travail, communiquer et promouvoir la collaboration documentaire	Secrétaire Responsable confirmée I	01	✓ Certifications utiles : **MOOC Gestion documentaire,** Certification Microsoft 365 / Google Workspace, Records Management / DPO ✓ Expérience sur SharePoint, Teams, OneDrive, Google Workspace, Dropbox Business, Alfresco, Nextcloud, etc. ✓ Avoir déjà accompagné la mise en place ou l'optimisation d'un système de gestion documentaire ✓ Avoir formé sur l'utilisation d'outils collaboratifs (OneDrive, SharePoint, Teams, Google Drive…) ✓ A l'aise à la structuration documentaire, cycle de vie, droits d'accès, versionning, métadonnées, normes (ISO 15489)
04	**GERER LES REUNIONS DE SUIVI DE PROJET ET LA DOCUMENTATION ASSOCIEE**	• Structurer, organiser et valoriser l'information dans l'organisation, couvrant les enjeux du cycle de vie documentaire (« GED », archivage, plan de classement, outils collaboratifs…) • Apporter des méthodes concrètes, des outils opérationnels et une vision stratégique adaptée aux besoins métier	Secrétaire Responsable confirmée I	01	✓ Certifications utiles : PMI-CAPM, PMP, Prince2, PM², Agile PM ✓ Avoir déjà conduit ou accompagné des projets complexes ✓ Savoir structurer un projet : jalons, livrables, responsabilités, délais, outils de pilotage (Gantt, RACI, etc.) ✓ Maîtriser la gestion des réunions, du temps et des parties prenantes ✓ Être capable d'enseigner une méthode adaptable : projets IT, RH, infra, transformation, etc.
05	**FORMATION OUTLOOK – REUNIONS, AGENDA, TACHES**	• Maîtriser l'interopérabilité entre messagerie, calendrier, tâches, contacts • Structurer les rendez-vous, événements, réunions, agendas partagés • Gérer les contacts, déléguer et suivre les tâches via tableaux de bord Outlook	Secrétaire Responsable confirmée I	01	✓ Parfaite connaissance des fonctions Agenda, Planification, Tâches, Groupes, Rappels, Catégories, Délégation ✓ Avoir déjà animé des formations bureautiques + organisation / gestion du temps ✓ Maîtrise à la fois les fonctions Outlook et la logique d'efficacité personnelle ✓ À l'aise en présentiel, distanciel, et support technique
06	**GESTION DES PRIORITES ET DES URGENCES**	• Comprendre son propre rapport au temps et identifier ses rythmes • Différencier urgences et priorités Identifier les tâches chronophages, optimiser sa disponibilité • Apprendre à déléguer et dire « non » • Se doter d'une organisation personnelle performante sur le moyen/long terme	Secrétaire Responsable confirmée I	01	✓ Time management, gestion du stress, certifications en productivité (ex. GTD) ✓ Maîtrise d'outils de hiérarchisation : matrice Eisenhower, loi de Pareto, ABCDE, impact/urgence, etc. ✓ Avoir déjà accompagné des professionnels en gestion du temps, efficacité personnelle, priorisation ✓ Capable d'adapter les outils à des contextes variés (terrain, bureau, distanciel, management)

LOT 3 : FORMATIONS MANAGERIALES

N°	THEME DE FORMATION	OBJECTIFS DE COMPETENCES	PUBLIC CIBLE	EFFECTIF	FORMATEUR
01	**CGEIT® – CERTIFIED IN THE GOVERNANCE OF ENTERPRISE IT**	• Définir et piloter un cadre stratégique de gouvernance IT • Aligner la gouvernance IT avec la stratégie d'entreprise • Gérer les ressources et investissements IT pour générer des bénéfices mesurables • Identifier et maîtriser les risques liés à l'infrastructure SI	PMO	01	✓ Certifications Recommandées : **CGEIT** + COBIT 2019 + éventuellement CISA ou CISM ✓ Expérience de 10+ ans dans l'animation de formations certifiantes ou de haut niveau : CGEIT, CISA, COBIT, ISO 27001, PMP, etc. ✓ Certification ou connaissance de COBIT 2019, ISO/IEC 38500, ITIL, ISO 27001, NIST (Atout) ✓ Avoir occupé des fonctions de gouvernance IT, DSI, RSSI senior, consultant en stratégie numérique ou en tant que consultant ✓ Capable de relier la théorie à la stratégie métier, la conformité, la valeur, et les risques

02	**MOP®, P3O®, PFMP®, PGMP®, SAFE AGILIST**	• Acquérir une compréhension complète du pilotage par portefeuille : principes, cycles de vie, pratiques, techniques et rôles associés • Savoir aligner projets/programmes/investissements sur les objectifs stratégiques de l'organisation • Optimiser la prise de décision, la gouvernance et l'allocation des ressources • Prévoir les bénéfices et supprimer les initiatives redondantes • Comprendre et interagir efficacement avec le modèle P3O® • Saisir la création, les rôles, services et fonctions des bureaux supports (PMO) à tous les niveaux • Savoir concevoir, mettre en place et piloter un P3O adapté au contexte organisationnel incluant gouvernance des investissements, alignement stratégique, optimisation des décisions • Démontrer une capacité avancée à gérer plusieurs projets et programmes alignés sur les objectifs stratégiques • Balancer et prioriser les demandes, piloter le succès du portefeuille, allouer les ressources judicieusement • Gérer des programmes complexes (ensembles de projets interconnectés) conformément aux objectifs stratégiques • Superviser les interdépendances, les risques, les parties prenantes, les bénéfices et la réalisation des objectifs via des programmes intégrés • Appliquer les principes Lean-Agile dans un contexte d'entreprise (cadre SAFe) • Diriger des transformations Lean-Agile et des PI Planning, encourager une mentalité Lean-Agile en tant que leader	PMO	01	✓ Certifié MoP® Practitioner obligatoire Expérience en gestion de portefeuille de projets (PMO, DSI, direction stratégie) Maîtrise du référentiel AXELOS (MoP, MSP, PRINCE2) ✓ Certifié P3O® Practitioner Expérience dans le déploiement ou pilotage de bureaux de projet (PMO, PgMO, CoE) Bonne connaissance des rôles et structures de gouvernance projet ✓ Certifié PfMP® en cours de validité Expérience significative (>8 ans) en management de portefeuille stratégique Parfaite maîtrise du Standard for Portfolio Management (PMI) ✓ Certifié PgMP® en cours de validité Expérience en gestion de programmes complexes Bonne pédagogie pour expliquer les logiques d'intégration, interdépendances et bénéfices ✓ Certifié SAFe® Agilist (SA) ou SPC (Program Consultant) Avoir animé des transformations agiles à l'échelle Expérience avec les rôles (RTE, Product Manager, ART, etc.)

03	**ARCHITECTURE DES SI – CONCEPTS FONDAMENTAUX / URBANISATION DU SI**	• Maîtriser les notions essentielles de l'architecture d'entreprise et du SI • Préciser le rôle, responsabilités et offre de l'architecte SI • Modéliser l'entreprise et son SI • Comprendre l'importance de l'architecture dans la gouvernance et piloter un projet d'architecture SI	PMO	01	✓ Certifications Recommandées : **TOGAF® (Foundation et Practitioner)/A**rchiMate®/DASA DevOps/SAFe Architect ✓ Maitrise claire des notions : couche métier, fonctionnelle, applicative, technique, cartographie, alignement SI/métier ✓ Expérience 10+ ans confirmés en architecture d'entreprise, urbanisation ou transformation du SI ✓ Bonne connaissance des systèmes d'information en silo, des schémas directeurs, et des projets SI métiers ✓ Savoir traduire des concepts techniques en enjeux métiers pour un public transversal
04	**ISO/IEC 27005 RISK MANAGER / EBIOS RM (ANSSI)**	• Expliquer les concepts et principes du management des risques en cybersécurité • Mettre en place, maintenir et améliorer un dispositif de gestion des risques adaptés au contexte organisationnel • Appliquer les processus ISO/IEC 27005 pour l'identification, l'analyse, l'évaluation, le traitement, la communication et le suivi des risques • Planifier et exécuter les actions de consultation et communication autour des risques informationnels • Approprier les enjeux de la cybersécurité par une méthode structurée, en combinant conformité et scénarios d'attaque CSB • Utiliser une démarche en ateliers (cadrage, identification des événements redoutés, scénarios stratégiques et opérationnels, traitement du risque • Comprendre le vocabulaire, les concepts développés par l'ANSSI et la compatibilité d'EBIOS RM avec ISO 27005 et ISO 31000 • Mener une étude complète des risques cyber en contexte professionnel	Responsable de la Sécurité du Système d'information	01	✓ Certifications Recommandées **: ISO 27001 Lead Implementer/Auditor, ISO 27005 Risk Manager**, EBIOS RM (Atout) ✓ Expérience de 10+ ans dans l'animation de formations certifiantes ✓ Avoir participé à des projets de SMSI et à l'évaluation de risques pour des organismes. ✓ Maîtrise des normes ISO 27001, 27002, 27005, 31000

05	**CERTIFIED INFORMATION MANAGEMENT PROFESSIONAL (CIMP)**	• Valider la compréhension approfondie des fondamentaux et disciplines spécifiques de la gestion de l'information. • Tester des connaissances opérationnelles avancées appliquées à chaque discipline (par ex. gouvernance des données, modélisation, qualité…) • Accéder au niveau CIMP Ex (niveau Expert) en combinant : formation académique (cours + examens dans un track), expérience pratique (minimum 5 ans dans le domaine), et excellentes performances aux examens (score moyen ≥ 75 %)	Responsable des Données, Transformation et Performance Ingénieur Principale des Données	02	✓ Certifications recommandées : **CIMP certifié dans une ou plusieurs filières (Data Governance, Data Quality, Metadata, MDM, etc)** ✓ Praticien senior en gouvernance ou gestion des données ✓ Notions de données sensibles, gouvernance réglementaire (RGPD, ISO 8000, ISO 27001), politiques d'usage, etc. ✓ Expérience confirmée en accompagnement de programmes de transformation data ✓ Bonne maîtrise des cadres méthodologiques (DMBOK, ISO 8000, EDM Council DCAM, etc.)
06	**CERTIFIED DATA MANAGEMENT PROFESSIONAL (CDMP)**	• Gouvernance des données • Métadonnées & données de référence • Qualité des données • Architecture des données • Intégration et interopérabilité • Sécurité des données • Modélisation et conception des données • Associate : réussir l'examen « Data Management Core » (minimum 60 %) — accessible dès 6 mois d'expérience en gestion des données • Practitioner : réussir l'examen de base et deux examens spécialisés (70 % minimum) avec 2 à 10 ans d'expérience • Mastery : réussir les examens de base et deux spécialisés (80 % minimum) avec au moins 10 ans d'expérience, plus étude de cas	Responsable des Données, Transformation et Performance Ingénieur Principale des Données	02	✓ Certifications recommandées : **CDMP (au moins Associate) Practitioner ou Master** ✓ Connaissance des enjeux RGPD, ISO 8000, FAIR, DCAM, ISO 27001, ainsi que des tendances (Data Mesh, IA, ESG, etc.) ✓ Avoir déjà animé des formations ou accompagnements en stratégie data, gouvernance, architecture, qualité ou MDM ✓ Expert en gouvernance des données, architecture d'entreprise, ou gestion de la qualité ✓ Bonne connaissance des standards ISO, réglementations, modèles sectoriels ✓ A l'aise avec la terminologie anglaise et l'animation de formations certifiantes
07	**METHODES AGILES DE DEVELOPPEMENT LOGICIEL POUR LES SI**	• Décrire la différence entre approches traditionnelles (prédictives) et approches agiles (adaptatives) • Mettre en œuvre les principales approches Agile (Scrum, Kanban, Lean…) • Présenter les techniques de base et expliquer leur application dans un projet • Comprendre la mise en œuvre de l'agilité dans le développement logiciel	Responsable du Génie Logiciel & Solutions	01	✓ Certifications recommandées : **Scrum Master** (CSM, PSM I ou II) Product Owner, SAFe Agilist, ICAgile, DevOps Foundation ✓ Expérience concrète en projets SI agiles ✓ Maîtrise des outils agiles : Jira, Trello, GitLab CI/CD, Confluence, etc. ✓ Capacité à faire le lien entre agilité, DevOps, qualité logicielle et gouvernance SI

LOT 4 : FORMATIONS TECHNIQUES

N°	THEME DE FORMATION	OBJECTIFS DE COMPETENCES	PUBLIC CIBLE	EFFECTIF	FORMATEUR
01	**MICROSOFT SC-200 / SC-300 / SECURITE MICROSOFT 365 & AZURE**	• Gérer un environnement de sécurité opérationnelle • Configurer protections et détections adaptées • Répondre efficacement aux incidents • Gérer les menaces de sécurité • Implémenter la gestion des identités (activités sur utilisateurs, groupes, rôles, attributs personnalisés) • Mettre en place l'authentification et la gestion des accès (MFA, Conditional Access, authentification SSO, réglementation d'accès) • Planifier et gérer les identités des workloads (applications, entités de service) • Déployer la gouvernance des identités (entitlement management, reviews des accès, PIM)	Ingénieur Sécurité du Système d'Information	01	✓ Certifications recommandées : **Certifié SC-200, SC-300, MS-500, AZ-500** ✓ Expérience Pratique : 7+ ans sur Microsoft Azure et 365 au minimum ✓ **Certifié Microsft Cerified Trainer** ✓ CISSP ou CCSP (Atout)
02	**SC-100 : MICROSOFT CYBERSECURITY ARCHITECT**	• Concevoir une stratégie de sécurité d'entreprise (Zero Trust) • Gouvernance, gestion du risque et conformité • Architecture de sécurité pour l'infrastructure • Stratégie de sécurité opérationnelle	Responsable de la Sécurité du Système d'information	01	✓ Certifications recommandées : **MCT, SC100**, AZ500, SC200, SC300, SC400, CISSP, CISM, CCSP ✓ Disposer d'une expérience 7+ans en cybersécurité et architecture.
03	**MICROSOFT CERTIFIED : AZURE SOLUTIONS ARCHITECT EXPERT**	• Conception des solutions Azure • Sécurité et gouvernance • Infrastructure & reseaux • **Plateforme applicative et DevOps** • Données et analytics • Monitoring et continuité	Responsable des Infrastructures, Réseaux et Support	01	✓ Certifications recommandées : **Microsoft Certified : Azure Solutions Architect Expert, Microsoft Certified Trainer,** AZ-305, AZ-104, AZ-500, AZ-400 ✓ Expérience Pratique : 5+ ans d'experience dans l'architecture et la mise en œuvre de solutions Azure, la gestion d'infrastructures hybrides et cloud, la sécurité, la gouvernance et la migration cloud ✓ CISSP ou CCSP (Atout)

04	**MICROSOFT AZ-500 : AZURE SECURITY TECHNOLOGIES**	• Gestion des identités et accès • Protection des plateformes • Sécurité des données et applications • Surveillance et réponse aux menaces	Responsable des Infrastructures, Réseaux et Support	01	✓ Certifications recommandées : **AZ-500, Microsoft Certified Trainer,** AZ-305, AZ-104, AZ-400 ✓ Expérience Pratique : 5+ ans d'experience dans l'architecture et la mise en œuvre de solutions Azure, la gestion d'infrastructures hybrides et cloud, la sécurité, la gouvernance et la migration cloud ✓ CISSP ou CCSP (Atout)
05	**SANS SEC530 : DEFENSIBLE SECURITY ARCHITECTURE AND ENGINEERING**	• Conception et architecture sécurisée • Sécurité réseau et segmentation • Protection des systèmes et des identités • Surveillance, détection et réponse • Sécurité du Cloud et environnements hybrids • Intégration dans les opérations et processus	Responsable des Infrastructures, Réseaux et Support	01	✓ Certifications recommandées : **GIAC Defensible Security Architecture (GDSA)** ✓ GIAC/SANS pertinentes (ex. GSEC, GCIA, GCIH, GCWN, GCPM, GCED, GCSA). ✓ Maintenir ses certifications et démontrer un apprentissage continu ✓ Expérience Pratique de formation en la matière 5ans minimum
06	**SANS INSTITUTE SEC545: GENAI AND LLM APPLICATION SECURITY**	• Maîtriser les fondamentaux de GenAI et des modèles de langage (LLMs) • Explorer les modèles, leurs ajustements et personnalisations • Identifier les risques spécifiques à GenAI et y répondre • Sécuriser les pipelines RAG, les embeddings et les bases de vecteurs • Mettre en œuvre des contrôles de sécurité dans les opérations GenAI (MLSecOps) • Comparer les options d'hébergement des applications GenAI • Utiliser les mécanismes de sécurité offerts par les clouds • Évaluer la sécurité des technologies adjacentes comme LangChain et les agents IA • Intégrer la sécurité GenAI dans un cadre organisationnel existant	Responsable de la Sécurité du Système d'Information	01	✓ Certifications recommandées : GWEB, GWAPT, OSWE, OSCP, CISSP, CISM ✓ Une expérience pratique avérée 5+ans en sécurité des applications et de l'IA/LLMs. ✓ Avoir reussi le processus interne sélectif SANS (audition + co-teaching).

07	**SAP SECURITY & AUTHORIZATIONS / AUDIT & COMPLIANCE IN SAP**	• Comprendre les fondamentaux de la sécurité SAP : utilisateurs, rôles, autorisations, politiques de mot de passe, SSO, cryptographie SSL/SNC, gestion des identités (SAP Identity Management), SAP GRC Access Control et gouvernance d'accès. • Sécuriser l'accès aux SAP NetWeaver (ABAP et Java), à SAP Fiori, BTP. • Mettre en place des pratiques de sécurité opérationnelle et de compliance (GDPR, audits…). • Déployer des solutions de GRC pour piloter la gestion des risques, la conformité réglementaire (SOX, GDPR, HIPAA), l'accès aux données, la séparation des tâches (Segregation of Duties). • Automatiser les audits, analyser les contrôles et fournir des rapports pour les équipes métiers et de conformité. • Former les auditeurs et responsables sécurité à comprendre l'écosystème SAP : modèles d'autorisation, analyses de risques SAP spécifiques, collaboration tri-ligne (TI, Ops, audit).	Responsable de la Sécurité du Système d'information	01	✓ Certifications recommandées : **C_SECAUTH_20 – SAP**, SAP Certified Application Associate – SAP Access**, SAP Certified Technology Specialist – SAP HANA, SAP Certified Basis Administrator**, ISO/IEC 27001 Lead Implementer ou Lead Auditor, ISO/IEC 27005 Risk Manager ou EBIOS RM ✓ 5+ ans d'expérience en formation sur SAP
08	**CLOUD SECURITY IMPLEMENTATION & DEVSECOPS**	• Comprendre et sécuriser les environnements cloud-native et DevOps via des pipelines automatisés • Intégrer la sécurité dans les CI/CD pipelines (scans de code, protection des secrets, contrôle des configurations) • Sécuriser les conteneurs et orchestrateurs Kubernetes, gérer la chaîne logistique logicielle (SBOM, signatures d'artefacts) • Automatiser la conformité et répondre aux incidents grâce à des politiques « policy-as-code »	Ingénieur Sécurité du Système d'Information	01	✓ Certifications recommandées **: CCSP,** DevSecOps Foundation / CDP, AZ-500 / AWS Security Specialty / CKS / Terraform Associate ✓ Bonne connaissance des normes ISO 27017/27018, NIST, CSA CCM, RGPD
09	**GESTION DU CYCLE DE VIE DES APPLICATIONS D'ENTREPRISE ET LEUR INTEROPERABILITE**	• Compréhension du cycle de vie applicative • Rationalisation et gouvernance des applications • Interopérabilité et integration • Convergence applicative et architecture cible • Sécurité et conformité • Gestion du changement et accompagnement	Responsable du Génie Logiciel et Solutions	01	✓ Certifications recommandées : COBIT 2019, CGEIT, ITIL 4 Managing Professional / Strategist, TOGAF, ArchiMate Certification, DevOps Foundation, DevSecOps Practitioner, PMI-ACP, ISO 27001 Lead Implementer / Lead Auditor, CISSP, CCSP
10	**RATIONALISATION LOGICIELLE ET CONVERGENCE APPLICATIVE**	• Analyser et diagnostiquer le portefeuille applicatif • Maîtriser les méthodes de rationalisation logicielle • Concevoir une stratégie de convergence applicative • Piloter la gouvernance applicative • Accompagner la transformation et le changement	Responsable du Génie Logiciel et Solutions	01	✓ Certifiations recommandées : TOGAF/ArchiMate, COBIT 19, ITIL® 4 Managing Professional, PRINCE2® Practitioner, Azure Solutions Architect Expert/AWS Certified Solutions Architect – Professional/Google Cloud Professional Cloud Architect ✓ Expérience 5+ans en architecture d'entreprise, urbanisation ou gouvernance IT. ✓ Pratique de la convergence applicative dans des environnements complexes (banques, assurances, télécoms, administrations, multinationales)

11	**SECURITE DES API ET DES ARCHITECTURES APPLICATIVES**	• Prendre en main les outils pour concevoir, déployer et superviser des API REST dans un environnement sécurisé • Appréhender les menaces spécifiques aux API Identifier les vulnérabilités courantes et appliquer les protections adéquates • Maîtriser les bonnes pratiques de conception, de développement et d'architecture des APIs REST pour renforcer leur sécurité	Ingénieur Sécurité du Système d'Information	01	✓ Certifications recommandées : **CSSLP/OWASP Advanced Training** Cert. DevSecOps / Cloud Security (Atout) ✓ Expérience dans la conception, l'intégration et la sécurisation d'APIs REST, GraphQL, SOAP…. ✓ Bonne connaissance des normes ISO 27017/27018, NIST, CSA CCM, RGPD
12	**SECURISATION DU CYCLE DE VIE LOGICIEL (DEVSECOPS, CI/CD SECURISE)**	• Développer une vision globale de la sécurité dans un contexte DevOps • Mettre en place des environnements sécurisés et évolutifs • Sécuriser la chaîne de développement : CI/CD, chaîne d'approvisionnement logicielle (Supply Chain), posture de sécurité des développeurs, sécurité cloud et conteneurisation • Appliquer les principes DevSecOps au sein d'une culture Agile/DevOps transparente	Ingénieur Sécurité du Système d'Information	01	✓ Certifications recommandées : **DevSecOps / Cloud Security,** CSSLP (ISC²), AZ-400 / AWS DevOps Pro / CKS / Terraform Associate ✓ Bonne connaissance des normes ISO 27017/27018, NIST, CSA CCM, RGPD ✓ 5+ ans d'expérience en sécurité applicative, DevOps ou développement logiciel sécurisé. ✓ Maîtrise des pipelines CI/CD + intégration de sécurité outillée (SAST, DAST, Container Scan...). ✓ Connaissance des frameworks (Spring, .NET, Node.js, Django) et de leur sécurisation.
13	**SECURITE DES APPLICATIONS WEB (OWASP, WAF, ETC.)**	• Identifier les vulnérabilités courantes des applications web (OWASP Top Ten : XSS, injections, détournements de session…) • Comprendre le déroulement d'une attaque réelle et les mécanismes d'exploitation • Mettre en place des mesures de protection simples : HTTPS, durcissement des serveurs, hardening • Tester la sécurité (pentest, scanners, audit) et déployer des contre-mesures adaptées • Configurer un serveur web avec chiffrement SSL/TLS, utiliser outils d'analyse et d'attaque pour valider les protections	Ingénieur Sécurité du Système d'Information	01	✓ Certifications recommandées : **OSWE (Offensive Security Web Expert),** eWPTX / eWPT, CSSLP, GIAC GWAPT ✓ Expérience offensive et défensive en sécurité web. ✓ Capacité à faire des démonstrations en direct de failles (XSS, IDOR, RCE...). ✓ Pédagogie adaptée aux développeurs, pentesters, RSSI ou profils DevSecOps.
14	**GERER LA CONFIGURATION, L'EXPLOITATION ET LA SUPERVISION DES SYSTEMES APPLICATIFS ET BASES ANALYTIQUES**	• Maîtriser les concepts de supervision et d'observabilité, incluant métriques, logs et traces • Comprendre les enjeux de collecte et de stockage de données applicatives et systèmes • Pratiquer les outils open-source (Prometheus, Grafana, Elastic, Loki, Jaeger, OpenTelemetry…) • Analyser les impacts organisationnels liés à l'implémentation de l'observabilité moderne	Responsable des Données, Transformation et Performance	01	✓ Certifications recommandées : ITIL 4 Foundation, Linux LPIC-2 / RHCSA, Oracle DBA / Microsoft SQL Server, Zabbix Certified ✓ 7+ ans d'expérience en exploitation IT, bases analytiques, monitoring. ✓ Maîtrise des environnements on-premise et cloud (Azure, AWS, GCP). ✓ Capacité à combiner théorie et démonstrations réelles (dashboards, tuning, troubleshooting).

15	**ARCHITECTURE DATA LAKEHOUSE / DATA FABRIC**	• Comprendre l'intégralité du processus d'analytique : ingestion à exploitation des données dans un environnement Microsoft Fabric Lakehouse • Créer et ingérer des données dans un lakehouse Fabric, notamment via Azure Dataflows Gen2 et pipelines Data Factory • Utiliser Apache Spark, manipuler DataFrames, travailler avec des tables Delta Lake (création, versioning, streaming • Mettre en œuvre une architecture lakehouse en couches (bronze, silver, gold), approche "médaillon"	Responsable des Données, Transformation et Performance	01	✓ Certifications recommandées : **Azure Data Engineer (DP-203**), Google Professional Data Engineer, Databricks Lakehouse Fundamentals ✓ 5+ ans d'expérience dans la data engineering / data architecture ✓ Avoir déjà mis en œuvre ou audité une architecture Lakehouse ou Data Fabric ✓ Capacité à vulgariser des architectures complexes pour des profils techniques ET métiers
16	**SAP SUCCESSFACTORS – ADMINISTRATION & EXPLOITATION / RH DIGITAL**	• Configurer les permissions basées sur les rôles (role-based permissions) • Gérer les données des employés et leurs attributs dans HR Core • Déployer les fonctionnalités d'auto-service RH et les workflows • Administrer les processus d'onboarding, les événements RH et les politiques de données • Superviser la conformité, les règles de confidentialité et les processus de reporting RH	Responsable des Données, Transformation et Performance	01	✓ Certifications recommandées : **SAP Certified Application Associate – SAP SuccessFactors Employee Central** ✓ Maîtrise des modules : Employee Central, Recruiting, Performance & Goals, Learning, Compensation… ✓ Compréhension du modèle cloud, intégration avec SAP ERP ou S/4HANA, interfaces, authentification SSO ✓ 5+ ans d'expérience minimum sur SAP SuccessFactors ✓ Avoir déjà formé et accompagné des équipes RH dans le paramétrage et l'administration quotidienne ✓ Bonne capacité à illustrer les fonctionnalités RH par des cas concrets
17	**SAP HANA – INTERVENTION DE PREMIER NIVEAU**	• Identifier les concepts clés de SAP HANA, sa plateforme et ses technologies intégrées • Manipuler les différentes interfaces SAP HANA destinées aux développeurs et aux administrateurs • Expliquer les étapes d'une migration vers SAP HANA • Créer des modèles de données via les outils de modélisation intégrés • Construire des rapports basés sur ces modèles et gérer le chargement des données • Décrire les fonctions d'entrepôts de données (BW/4HANA, SQL Data Warehouse, SAP DWC) • Assurer la surveillance via SAP HANA Cockpit • Maintenir la sécurité et la confidentialité des données au sein de SAP HANA	Administrateur de base de données confirmé II Ingénieur Principale des Données	02	✓ Certifications recommandées **: SAP Certified Technology Associate**, SAP HANA 2.0 (C_HANATEC_18) (Atout) ✓ Maitrise de l'architecture HANA (nodes, services, système distribué, S/4HANA, HANA XS Engine) ✓ Savoir utiliser SAP HANA Cockpit, SAP HANA Studio, SAP HANA Database Explorer, SAP DBACOCKPIT ✓ 5+ans d'expérience technique sur SAP HANA ✓ Capacité à vulgariser pour des techniciens ou administrateurs non-spécialistes SAP

18	**MAITRISE DU VOLET FONCTIONNEL DE SAP**	• Acquérir les compétences métier indispensables à l'exploitation d'un environnement SAP fonctionnel • Maîtriser la navigation dans l'interface SAP, comprendre l'architecture et les modules ERP fondamentaux • Découvrir les principaux modules fonctionnels (SD, MM, WM, PP, PM, QM, FI, CO…) et leur interaction dans les processus métier • Acquérir les bases techniques complémentaires : langage SQL, notions d'ABAP, utilisation du débogueur SAP • Se familiariser avec la posture d'un consultant fonctionnel : approche projet, relation client, sens du conseil, conduite Agile/Scrum	Administrateur de base de données confirmé II	01	✓ Certifications recommandées : **SAP Certified Application Associate** ✓ Maitrise de l'interaction entre FI/CO, MM, SD, PP, HCM, etc. ✓ Maîtrise des processus financiers (FI/CO), logistiques (MM/SD/PP), RH (HCM/SF), achats, ventes, etc. ✓ Expérience significative (5 à 10 ans) dans 3+ modules SAP fonctionnels ✓ Avoir exercé comme consultant fonctionnel, key-user ou AMOA ✓ Bonne capacité à expliquer les processus métier et les refléter dans SAP
19	**TECHNIQUES DE REPLICATION, ETL/ELT ET SYNCHRONISATION DES DONNEES**	• Comprendre les concepts clés et l'architecture de Snowflake • Importer des données structurées et semi-structurées • Transformer les données au sein de Snowflake en utilisant pipelines (streams & pipes)	Administrateur de base de données confirmé II	01	✓ Certifications recommandées : **Azure Data Engineer (DP-203),** Google Data Engineer, Snowflake SnowPro Core / Advanced Data Engineer ✓ 5+ ans en data engineering, ETL/ELT, ou architecture d'intégration de données ✓ Maîtrise de plusieurs outils ETL/ELT (au moins un open-source, un cloud, une entreprise) ✓ À l'aise avec les approches traditionnelles (batch, ETL) et modernes (streaming, ELT, cloud-native)
20	**OUTILS D'ANALYSE DE PERFORMANCES SQL / TUNING**	• Décrire l'architecture interne de SQL Server et ses composants • Analyser le modèle d'exécution, les files d'attente et problème de goulots d'étranglement • Optimiser les performances I/O, mémoire, cache et TempDB • Diagnostiquer et corriger les problèmes de plan d'exécution (Optimizer, Query Store…)	Administrateur de base de données confirmé II	01	✓ Certifications recommandées : **Oracle Database Performance Tuning,** Microsoft DP-300 (Azure SQL), PostgreSQL Associate / Expert ✓ 5+ ans d'experience en tant que DBA, développeur SQL, data engineer ou consultant performance ✓ Environnements maîtrisés : au moins 2 moteurs SQL (ex : Oracle + PostgreSQL ou SQL Server + MySQL) ✓ Capacité à créer des démonstrations en direct de tuning (avant/après) ✓ Maitrise des outils de tuning natifs : ▪ Oracle AWR/ASH ▪ SQL Server Profiler / DMVs ▪ pg_stat_statements

21	**GERER LA CONFIGURATION, L'EXPLOITATION ET LA SUPERVISION DES SYSTEMES APPLICATIFS ET BASES ANALYTIQUES**	• Comprendre les concepts fondamentaux de l'observabilité : métriques, logs, traces • Maîtriser la génération, la collecte et le stockage de ces données • Connaître les outils de supervision/applicative les plus pertinents de l'écosystème Cloud Native (Prometheus, Grafana, Fluentd, Loki, OpenTelemetry, Jaeger…) • Appliquer ces technologies dans un contexte de systèmes distribués ou microservices • Anticiper les impacts organisationnels liés à l'architecture observabilité moderne	Responsable des Données, Transformation et Performance	01	✓ Certifications recommandées : ITIL 4 Foundation Linux LPIC / RHCSA Microsoft AZ-104 / AWS SysOps Admin Zabbix / Prometheus. ✓ 5+ ans d'expérience en administration ou le support infrastructure ou bases analytiques ✓ Maîtrise de plusieurs outils de supervision, scripts d'automatisation, bases de données
22	**INTEROPERABILITE ET ARCHITECTURE ORIENTEE DONNEES (DATA MESH, DATA FABRIC)**	• Acquérir les concepts fondamentaux du Domain-Driven Design, du Data Mesh, du Data Product et des Data Contracts • Aligner ces notions avec la gouvernance des données et savoir dresser une feuille de route pour le déploiement d'un projet Data Mesh • Prioriser les étapes, identifier les parties prenantes, choisir les outils adaptés • Construire une architecture technique et logique Data Mesh, intégrer une gouvernance fédérée • Identifier les mécanismes d'interopérabilité entre les Data Products et assurer la compatibilité ascendante, la conformité RGPD, la gouvernance des données	Données Transformation & Performance, Ingénieur Principale des Données	02	✓ Certifications recommandées : Azure Data Engineer (DP-203) Google Professional Data Engineer Databricks Lakehouse cert. ✓ 5+ ans d'expérience en architecture de données, intégration ou data gouvernance ✓ Avoir mené des projets d'urbanisation data, mise en place de MDM / data catalog, ou de modernisation vers le cloud ✓ À l'aise pour former aussi bien des architectes, des MOA/MOE, que des équipes métiers data owners
23	**CONCEPTION ET DEPLOIEMENT D'ARCHITECTURES DATA MODERNES**	• Comprendre le rôle de l'architecte de données et son interaction avec le Data Office, notamment la gouvernance et la conformité • Comparer différentes structures architecturales : data warehouse, data vault, data mesh, data lake, modern data stack • Décrire les schémas d'architecture adaptés, modéliser les données, choisir les outils pertinents selon les cas d'usage • Maîtriser le cycle de vie complet des données : ingestion, stockage, traitement, gestion des métadonnées, sécurité, sauvegarde, restauration • Mettre en œuvre une stratégie d'architecture de données alignée avec les objectifs métier et ROI	Données Transformation & Performance Ingénieur Principale des Données	02	✓ Certifications recommandées : Azure DP-203 Google Professional Data Engineer , SnowPro Advanced, Databricks Lakehouse ✓ 5+ ans d'expérience en architecture data / ingénierie des données ✓ Avoir déjà conçu ou déployé des plateformes analytiques d'entreprise

24	**SECURITE DES APPLICATIONS ET DEVSECOPS**	• Comprendre le cycle DevSecOps au sein d'environnements cloud et microservices conteneurisés • Intégrer la sécurité dès les premières phases de développement (shift-left), via des tests automatisés dans CI/CD • Planifier une transition d'une organisation DevOps vers DevSecOps • Intégrer des outils de sécurité (scanners de conteneurs, audits, SIEM) adaptés aux architectures actuelles	Responsable du Génie Logiciel et Solution	01	✓ Certifications recommandées : **DevSecOps Foundation / Practitioner, CSSLP, Certified DevSecOps Engineer (CDOE)** ✓ 5+ ans d'expérience en développement sécurisé, DevOps, ou cybersécurité applicative ✓ Avoir déjà mis en œuvre une chaîne DevSecOps complète dans un contexte réel (CI/CD, SAST/DAST, IaC) ✓ Capacité à former des profils mixtes (développeurs, DevOps, RSSI, architectes)
25	**OUTILS DE GESTION DES VULNERABILITES DANS LE CODE**	• Comprendre les fondements et outils DevSecOps adaptés à l'intégration de la sécurité dans les pipelines CI/CD • Identifier, analyser, prioriser et corriger les vulnérabilités dans le code source et les composants applicatifs • Mettre en pratique les outils modernes de détection, d'analyse et de remédiation des vulnérabilités • Aborder les enjeux organisationnels liés à la sécurisation du code	Responsable du Génie Logiciel et Solution	01	✓ Certifications recommandées : **CSSLP DevSecOps Practitioner**, eWPT / OSWE / Secure Code Warrior Certs ✓ Expérience significative en développement sécurisé, DevSecOps ou audit de code ✓ Maîtrise des principaux outils de scan open-source et commerciaux ✓ Capacité à former développeurs, DevOps, architectes ou équipes sécurité
26	**DEVELOPPEMENT ET SECURISATION DES APIS ET SERVICES WEB**	• Prendre en main les outils nécessaires à chaque phase du cycle de vie des API (conception, déploiement, supervision) • Identifier et comprendre les menaces spécifiques aux API exposées • Détecter les vulnérabilités courantes (injections, CSRF, mauvaises implémentations d'authentification…) • Mettre en œuvre les protections adéquates, incluant authentification (OAuth2, OpenID Connect), CORS, sanitization, logging • Appliquer les bonnes pratiques de conception, développement et architecture REST	Concepteur - Développeur confirmé II	01	✓ Certifications recommandées : **CSSLP,** eWPT / OSWE, DevSecOps Practitioner, **API Security Specialist (APIsec University)** ✓ Expérience équilibrée entre développement backend et cybersécurité applicative ✓ Capacité à expliquer à la fois comment construire une API et comment la protéger efficacement ✓ À l'aise pour former des développeurs, architectes, équipes sécurité / DevSecOps
27	**INTEGRATION CONTINUE ET TESTS D'INTEGRATION POUR LES API**	• Automatiser les tests d'API REST avancés. • Utiliser des frameworks tels que REST Assured pour écrire des tests automatisés d'API. • Intégrer ces tests dans un pipeline d'intégration continue (CI) pour validation automatisée des services Web.	Concepteur - Développeur confirmé II	01	✓ Certifications recommandées : **DevOps Foundation / Practitioner, API Test Engineer (ISTQB ou équivalent)** Postman Supernova / Expert ✓ 5+ ans d'expérience en développement backend, DevOps ou assurance qualité logicielle ✓ Avoir participé à des projets avec API exposées en production, et tests intégrés dans le CI/CD ✓ Capacité à former des profils mixtes (développeurs, testeurs, DevOps, sécurité)

28	**DEVSECOPS PRACTITIONER**	• Comprendre les principes avancés du DevSecOps et leur application dans une organisation • Distinguer les éléments techniques utilisés dans les pratiques DevSecOps (infrastructure, pipelines, observabilité…) • Appliquer les concepts de maturité numérique selon une approche people-process-technology • Mettre en place des indicateurs métriques adaptés à l'organisation pour mesurer maturité et progrès • Reconnaître et planifier les transitions d'architectures logicielles (monolithe → microservices…) • Comparer différentes infrastructures DevSecOps (PaaS, serveurless, event-driven…) • Intégrer la sécurité dans les pipelines CI/CD, y compris sécurisation de dépôts et de données • Mettre en œuvre des pratiques de monitoring et d'observabilité pour des retours exploitable DevOps Institute • Explorer les pratiques expérimentales (Chaos Engineering, "Third Way") pour améliorer résilience et qualité • Identifier les tendances émergentes dans le domaine DevSecOps pour anticiper les évolutions	Concepteur - Développeur confirmé II	01	✓ Certifications recommandées : **DevSecOps Practitioner**, CSSLP / CCSP / OSWE / CDOE ✓ Connaissance des référentiels et cadres normatif OWASP SAMM, NIST SSDF (SP 800-218), ISO 27034, CIS Controls ✓ 5 à 10 ans d'expérience en DevOps, développement sécurisé ou cybersécurité applicative ✓ Avoir piloté des projets DevSecOps, y compris avec des pipelines CI/CD, conteneurs et intégrations de tests sécurité ✓ Capable de former des publics techniques avancés, dans des contextes réels (secteurs régulés, cloud, etc.)
28	**UTILISATION DE GIT, DOCKER, OUTILS DE TESTS AUTOMATISES**	• Maîtriser Git pour le versioning, la gestion des branches, les sous-modules, l'historique, workflows GitFlow • Utiliser Docker pour automatiser le déploiement des applications conteneurisées • Mettre en place des pipelines CI/CD avec GitLab (GitLab CI) pour les besoins DevOps automatiques	Concepteur - Développeur confirmé II	01	✓ Certifications recommandées : Docker Certified Associate, GitHub Actions, ISTQB Automation Engineer ✓ 5+ans d'expérience dans le développement logiciel / DevOps / automatisation de tests ✓ Maîtrise complète de l'enchaînement code → commit → build Docker → tests → rapport ✓ Capable de former des profils confirmés, développeurs ou QA technique
29	**SYSTEMES DE LOGS ET FORMATS (SYSLOG, JSON, CEF, ETC.)**	• Syslog : collecte centralisée, architecture, parsing, routage ; • Formats de logs structurés : JSON (logs structurés, ELK stack ingestion), CEF (Common • Event Format, utilisé avec ArcSight ou IBM QRadar) ; • Outils SIEM : ingestion de logs multiples (textuels, JSON, CEF), normalisation, corrélation, alerting.	Concepteur - Développeur confirmé II	01	✓ Certifications recommandées : GCIA / GCLD (GIAC), Splunk / ELK certs, ISO 27001 / SOC Analyst certs ✓ 5+ ans d'expérience en administration système, sécurité opérationnelle (SOC) ou ingénierie log/SIEM ✓ Maîtrise des formats, protocoles, outils de collecte et d'analyse ✓ Capacité à former des profils techniques et analystes (admin système, SOC, développeurs, etc.)

30	**CLOUD NETWORKING (AZURE, AWS OU GCP)**	• Configuration réseaux virtuels : VPC/AWS, Virtual Network/Azure, VPC/GCP, gestion des services réseau (sécurité, réseaux, connectivité hybride/multi-cloud, VPN, ExpressRoute, Direct Connect, peering), sécurité cloud : IAM, chiffrement, bonnes pratiques réseaux, conformité, conception d'architectures robustes, sécurisées, optimisées multicouches réseaux et multi-cloud.	Ingénieur Principal réseaux	01	✓ Certifications recommandées : AWS Advanced Networking – Specialty, **Azure Network Engineer Associate**, Google Professional Cloud Network Engineer ✓ 5+ ans d'expérience en réseau et infrastructure cloud ✓ Avoir exercé en tant que Cloud Network Engineer, Architecte Cloud ou Consultant Infrastructure
31	**CISCO CCNP SECURITY**	• Maîtriser les principes fondamentaux de la sécurité des réseaux • Configurer et gérer les pares-feux Cisco pour le contrôle d'accès • Déployer des solutions de sécurité de la messagerie, du web et DNS • Implémenter des solutions de VPN et de contrôle d'accès à distance • Comprendre la sécurité des terminaux, du cloud et la surveillance réseau • Se préparer à la certification Cisco SCOR et CCNP Security	Ingénieur Principal réseaux	01	✓ Certifications recommandées **Cisco CCNP Security à jour**, Certifié CCNP Security, CCIE Security ✓ 5+ ans d'expérience en ingénierie réseau sécurité, déploiement Cisco, ou SOC avec Cisco
32	**MICROSOFT CERTIFIED : AZURE NETWORK ENGINEER ASSOCIATE**	• Concevoir, mettre en œuvre et gérer des infrastructures réseau de base dans Azure (VNets, adresses, DNS, routage) • Déployer et administrer des services de connectivité réseau (VPN, ExpressRoute), Implémenter des services d'équilibrage de charge et de livraison d'applications (Load Balancer, Application Gateway, Front Door) • Garantir la sécurité réseau via NSG, Azure Firewall, WAF, DDoS Protection, etc., • Offrir des accès privés aux services Azure via Private Link, Private Endpoints ou Service Endpoints • Mettre en place des mécanismes de surveillance et de diagnostic réseau (Azure Monitor, Network Watche	Ingénieur Principal réseaux Technicien Télécom et Réseau confirmé II	02	✓ Microsoft Certified : **Azure Network Engineer Associate (AZ-700),** AZ-104 (Azure Administrator), AZ-305 (Solutions Architect), SC-100 (Cybersecurity Architect) ✓ 5+ ans d'expérience dans le déploiement de solutions réseau Azure ✓ Avoir déjà formé ou accompagné des architectes cloud, des ingénieurs réseau ou des exploitants Azure
33	**CISCO CERTIFIED DESIGN EXPERT (CCDE)**	• Élaborer des architectures réseau stratégiques alignées aux objectifs métier • Concevoir des solutions complexes multi-domaines et multi-technologies • Optimiser la gouvernance technique et la prise de décision en architecture • Appliquer les meilleures pratiques de design à grande échelle (scalabilité, disponibilité, sécurité, performance) • Gérer l'évolution, la migration et la transformation d'architectures réseau • Documenter et défendre les solutions d'architecture dans des scénarios complexes	Ingénieur Principal réseaux	01	✓ Certifications recommandées : **CCDE**, CCIE Routine & Switching/Enterprise + architecte confirmé ✓ Avoir conçu des architectures réseau critiques dans des environnements grands comptes, datacenters, hybrides ou cloud ✓ À l'aise avec les modèles d'architecture métier et la gouvernance technico-financière

34	**ARCHITECTURE RESEAU MODERNE ET SOFTWARE DEFINED NETWORKING (SDN)**	• Comprendre les fondements fonctionnement du SDN, architecture par programmation centralisée via un contrôleur • Maîtriser les bénéfices applicatifs et les usages du SDN • Avoir une vision claire des différents réseaux couverts par le SDN • Évaluer les possibilités de virtualisation des réseaux	Ingénieur Principal réseaux	01	✓ Certifications recommandées : Cisco Certified DevNet Professional / CCNP Enterprise + ENSLD, VMware VCAP-NV, Juniper JNCIS-SP/ENT ✓ 5+ ans d'expérience en ingénierie ou architecture réseau ✓ Expérience pratique avec au moins une plateforme SDN (Cisco ACI, NSX, Contrail…)
35	**FONDAMENTAUX CYBERSECURITE RESEAU (SECNUMACAD, ISO 27001 BASE)**	• Acquérir les notions de base de la cybersécurité • Connaître les risques numériques et comment protéger ses usages • Sensibiliser sans expertise technique préalable • Acquérir une compréhension de la norme ISO 27001 • Apprendre à définir un SMSI conforme	Technicien Télécom et Réseau confirmé II	01	✓ Certifications recommandées : **ISO/IEC 27032 Lead Cybersécurity Manager, ISO 27001 Lead Implementer/ Foundation,** SecNumAcad, CompTIA Security+, ANSSI ou MOOC CNIL ✓ 5+ ans d'expérience en cybersécurité ou administration réseau avec volet sécurité ✓ Expérience en formation ou vulgarisation SSI (animation de sessions de sensibilisation) ✓ À l'aise avec les référentiels français (ANSSI) et internationaux (ISO)
36	**SECURITE DES ECHANGES INTER-APPLICATIFS (VPN, PARE-FEUX, ACL, DMZ)**	• Comprendre les principes de fonctionnement d'un firewall • Mettre en œuvre différentes solutions du marché • Appréhender les dispositifs d'authentification/autorisation (AAA) • Configurer des VPN IPSec site-à-site et distants • Gérer les ACL, NAT, DMZ et architectures sécurisées selon les recommandations ANSSI	Technicien Télécom et Réseau confirmé II	01	✓ Certifications recommandées : **Cisco CCNP Security / CCNA Security,** CompTIA Security+, Fortinet NSE4, ISO 27001 Foundation ✓ 5+ ans d'expérience en sécurité réseau ou infrastructure ✓ Avoir déjà mis en œuvre des architectures sécurisées (DMZ, VPN, firewalling, reverse proxy) ✓ À l'aise pour illustrer les schémas de flux réseau et expliquer les décisions d'architecture
37	**VOIP ET COMMUNICATIONS UNIFIEES (MICROSOFT TEAMS, CISCO CUCM)**	• Concevoir et déployer des solutions de communications unifiées Cisco (CUCM, BE6000, téléphone IP, messagerie unifiée) • Installer, administrer et dépanner les équipements et protocoles de téléphonie (SIP, MGCP, SCCP) • Intégrer la signalisation, la messagerie instantanée, la présence, la téléphonie vidéo	Technicien Télécom et Réseau confirmé II	01	✓ Certifications recommandées : **Cisco CCNP Collaboration**, Microsoft Teams Voice Engineer, Associate (MS-720), CompTIA CTP+ (VoIP) ✓ Expérience de 5+ ans avec la VoIP, la collaboration d'entreprise ou l'exploitation de plateformes UC ✓ Avoir déjà déployé Cisco CUCM ou Microsoft Teams Voice avec PSTN ✓ À l'aise avec les interconnexions hybrides, la sécurité VoIP et la qualité de service

38	**FORTINET NSE1–NSE4**	• Identifier les acteurs malveillants, leurs motifs, et les techniques d'attaque • Comprendre les impacts des attaques sur les responsables (CIO, CISO, CFO) • Connaitre les stratégies de sécurité personnelle en ligne et les termes clés du domaine • Visualiser l'évolution des menaces et besoins en sécurité • Prendre conscience des stratégies défensives modernes • Connaître l'écosystème de produits Fortinet (FortiGate, FortiMail, FortiAnalyzer…) • Comprendre les cas d'usage et synergies entre outils • Installer, configurer et assurer les opérations quotidiennes sur FortiGate • Maîtriser les politiques de sécurité, VPN, profils inspection, HA	Technicien Télécom et Réseau confirmé II	01	✓ Certifications recommandées : **NSE 4**, CompTIA Security+, CEH, ISO/IEC 27001 Foundation/Lead Implementer, Cisco CCNP Security ✓ Avoir déjà déployé ou administré des équipements Fortinet (FortiGate, FortiAnalyzer, VPN, filtrage, UTM, HA)
39	**VIRTUALISATION SOUS VMWARE ET HYPERV**	• Comprendre les concepts de base de la virtualisation • Maîtriser l'installation et la configuration de VMware vSphere et Hyper-V	Technicien maintenance et support Confirmé II Responsable des Infrastructures, Réseaux et Support	02	✓ Certifications recommandées : **VMware VCP-DCV (Professional),** Microsoft Certified : Windows, Server Hybrid Administrator Associate, CompTIA Server+ ✓ Expérience dans la virtualisation serveur & infrastructure ✓ Avoir travaillé sur des environnements vSphere et Hyper-V, y compris stockage partagé, clustering, sauvegarde
40	**GESTION AZURE AD**	• Explorer les concepts d'identité dans Azure AD • Configurer et gérer les identités dans Azure AD, y compris hybrides et externes • Mettre en œuvre l'authentification multifacteur (MFA), accès conditionnel, protection identités • Assurer l'intégration et le SSO des applications, l'enregistrement d'applications • Mettre en œuvre des politiques de gouvernance d'accès, droits privilégiés, revues d'accès • Surveiller et maintenir Azure AD via journaux et alertes	Technicien maintenance et support Confirmé II	01	✓ Certifications recommandées **: SC-300 : Microsoft Identity and Access Administrator**, MS-500 ou AZ-104 ✓ 5+ ans d'expérience en gestion d'identité cloud / hybride, notamment sur Azure AD ✓ Avoir déjà animé des formations sur Microsoft 365, Azure ou la cybersécurité des identités

41	**MICROSOFT 365 CERTIFIED: MODERN DESKTOP ADMINISTRATOR ASSOCIATE**	• Déployer Windows (15–20 %) : installation, mise à niveau, migration et activation de Windows, personnalisation après l'installation. • Gérer les appareils et les données (35–40 %) : gestion des utilisateurs/groupes, permissions NTFS, stratégies locales, sécurité du pare-feu Windows Defender, chiffrement, etc. • Configurer la connectivité (15–20 %) : configuration du réseau IP, VPN, Wi-Fi, PowerShell à distance, Bureau à distance. • Maintenir Windows (25–30 %) : récupération du système, restauration de fichiers (OneDrive), mise à jour de Windows, surveillance des journaux et gestion de la performance.	Technicien maintenance et support Confirmé II	01	✓ Certifications recommandées : **MD-100 + MD-101 (ou MD Associate obtenu),** AZ-104, MS-500 ou SC-300 ✓ Avoir géré des projets de migration, déploiement, sécurisation ou support Windows/M365 ✓ À l'aise avec Intune, Azure AD, scripts, outils Microsoft 365
42	**GESTION DE PARCS INFORMATIQUES MODERNES (SCCM, INTUNE)**	• Intégrer Microsoft Endpoint Manager / SCCM pour gérer de manière unifiée les PC et appareils mobiles • Maîtriser l'inventaire logiciel et matériel, les déploiements d'applications, la gestion de configuration • Automatiser l'installation et les mises à jour des postes de travail • Superviser et maintenir l'infrastructure SCCM	Technicien maintenance et support Confirmé II	01	✓ Certififcations recommandées : MD-101 Managing Modern Desktops**, Microsoft Certified : Endpoint Administrator Associate,** AZ-104 ✓ Avoir déployé ou administré SCCM et/ou Intune dans des environnements de production ✓ Être Capable de démontrer la cohabitation ou migration d'un modèle SCCM vers Intune
43	**CONNAISSANCES DE BASE EN CYBERSECURITE (SECNUMACAD, ANSSI)**	• Panorama de la sécurité des systèmes d'information – acteurs, enjeux et menaces numériques • Sécurité de l'authentification – bonne gestion des mots de passe, authentification sécurisée • Sécurité sur Internet – navigation, messagerie, menaces web et précautions de base • Sécurité du poste de travail et nomadisme – protections de l'ordinateur, usage nomade et bonnes pratiques numériques	Technicien maintenance et support Confirmé II	01	✓ Certifications recommandées **: SecNumAcad** (validé l'attestation), ISO/IEC 27001 Foundation ou Lead Implementer, CEH, Security+, CISSP (Atout)
44	**SURVEILLANCE ET GESTION DE LA PERFORMANCE RESEAU DANS UN SI COMPLEXE**	• Définir une stratégie d'administration réseau efficace • Utiliser des outils Open Source (Nagios, SNMP, MRTG, SmokePing, Nmap, AIDE) • Superviser les performances réseau et garantir la disponibilité	Administrateur de base de données confirmé II Technicien Télécom et Réseau confirmé II	02	✓ Certifications recommandées : **CCNP Enterprise/Network Monitoring**, Fortinet NSE, CompTIA Network+, AWS Networking ✓ Avoir mis en place ou administré des outils de supervision (Nagios, Centreon, Zabbix, etc.) ✓ Bon bagage théorique + pratique sur les performances réseau

45	**OUTILS DE SUPERVISION (NAGIOS, ZABBIX, PRTG, ETC.)**	• Installer, configurer et administrer un système de supervision robuste sous Nagios (ou Centreon, Cacti). • Comprendre les principes fondamentaux : SNMP, définition des cibles, alertes personnalisées et visualisation des performances. • Mettre en place des graphes de performance et anticiper les incidents. • Appréhender les principes de supervision : protocoles (HTTP, SMTP, POP3, PING…), ressources à surveiller. • Installer et configurer Zabbix, déployer les agents, automatiser la découverte de serveurs. • Mettre en œuvre des alertes personnalisées, corrélations, SLA, actions automatisées et visualisation via graphiques. • Maîtriser l'outil PRTG : alertes réseau, surveillance de la performance, optimisation de la bande passante. • Configurer des rapports, dashboards personnalisés, gérer incidents de sécurité réseau.	Technicien Télécom et Réseau confirmé II	01	✓ Certifications recommandées : Zabbix Certified Specialist / Professional, Formations Nagios/PRTG ✓ Expérience opérationnelle sur au moins 2 outils (ex : Zabbix + PRTG, ou Nagios + Centreon) ✓ Avoir déjà déployé des sondes réseau, systèmes, bases de données ou applicatives ✓ À l'aise avec les protocoles SNMP, ICMP, WMI, API REST, syslog, traps
46	**ADVANCED NETWORKING (CISCO, JUNIPER) / SDN & NETWORK AUTOMATION**	• Comprendre le rôle de l'automatisation programmée dans la gestion réseau • Définir les méthodes DevOps/NetDevOps appliquées aux réseaux • Développer des automations basées Python (scripts HTTP/API, RESTCONF, NETCONF, Ansible) • Manipuler YANG, Jinja2, YAML, JSON, XML frameworks Elaborer des playbooks Ansible pour configurer des services réseaux	Technicien Télécom et Réseau confirmé II	01	✓ Certifications recommandées : **Cisco CCNP / CCIE**, Juniper JNCIP / JNCIE, DevNet Professional, NSX-T, ACI Specialist, SD-WAN ✓ 5+ ans d'expérience pratique sur infrastructures réelles Cisco/Juniper ✓ À l'aise avec la configuration réseau et infrastructure as code
47	**CISCO ISE CONFIGURATION AND DEPLOYMENT**	• Décrire Cisco ISE, son architecture et ses modèles de déploiement • Mettre en œuvre les composants de contrôle d'accès et configurer les politiques (MAB, 802.1X) • Dépanner les politiques ISE et le support d'équipements NAD tiers • Configurer l'accès invité, les portails hotspot et les services BYOD • Configurer les services de posture (endpoint compliance) et posture-based access • Gérer TACACS+ pour l'administration des équipements réseau ISE • Comprendre et configurer Cisco TrustSec pour segmenter le réseau • Maîtriser les services de profiling (Cisco ISE Profiler) et leur exploitation via rapports et bonnes pratiques	Technicien Télécom et Réseau confirmé II	01	✓ Certifications recommandées : Cisco CCNP Security, **Cisco ISE Specialist**, CCIE Security ✓ Avoir déjà déployé Cisco ISE dans un environnement en production ✓ A l'aise avec les flux RADIUS, les VLAN dynamiques et les politiques d'accès ✓ Dispose d'un environnement lab (EVE-NG, CML, GNS3, VirtualBox) prêt à l'emploi pour les simulations

EVALUATION DES OFFRES

CRITERES ADMINISTRATIFS

DETAILS DES CRITERES	STATUT	NOTE
La lettre de soumission à l'appel d'offres	Obligatoire	/2
Le chiffre d'affaires du dernier exercice clos	Exigé	/2
La localisation précise du siège social de l'entreprise (plan de localisation)	Exigée	/1
Certificat d'inscription au Registre de Commerce et du Crédit Mobilier (RCCM)	Obligatoire	/3
Attestation en cours de validité certifiant que le soumissionnaire est en règle vis-à-vis de l'administration fiscale	Exigée	/3
Déclaration Fiscale d'Existence (DFE)	Obligatoire	/2
Attestation en cours de validité certifiant que le soumissionnaire est en règle vis-à-vis de la Sécurité Sociale	Exigée	/3
Curriculum vitae des principaux dirigeants	Exigé	/2
Assurance responsabilité Civile de l'entreprise	Obligatoire	/2
TOTAL (NOTE_AD)		**/20**

CRITERES TECHNIQUES

LIBELLE DES CRIERES	DESCRIPTION	IMPORTANCE	NOTE
Présentation de l'offre	L'offre devra être présentée de façon propre, lisible, paginée avec sommaire et facilement exploitable. L'évaluation tient compte de la disponibilité et la conformité des pièces administratives.	Départageant	/5
Expérience générale du cabinet de formation dans la formation continue	Il s'agit des références du soumissionnaire dans le domaine de la formation professionnelle continue. Il faudra tenir compte du nombre d'années d'existence de l'organisme de formation et de ses diverses expériences en formations développées dans sa présentation.	Départageant	/5
Les références techniques (attestations de bonne exécution)	Le soumissionnaire doit fournir dans son offre les attestations de bonne exécution (ABE) relatives aux thèmes auxquels il fait référence. Des ABE doivent être produites pour chaque action de formation envisagée.	Départageant	/10
Qualifications générales du formateur (Niveau / diplôme)	Il s'agira d'examiner les qualifications du formateur (diplômes, certificats, CV, etc..) pour juger son niveau de qualification.	Départageant	/15

Qualifications spécifiques du formateur (diplômes, certificats, années d'expérience dans le domaine)	Il s'agira d'examiner les qualifications spécifiques (diplômes, certificats, CV) du formateur dans le domaine de la formation sollicitée pour juger son aptitude à animer la formation.	Départageant	/20
Conformité de l'offre	Ce critère examine la conformité entre l'offre du soumissionnaire, les objectifs et résultats attendus dans le cahier des charges.	Départageant	/10
Méthodes, contenus et supports proposés	La méthode pédagogique, fiche technique, le support de formation et la durée de formation devront être présentées de façon propre, lisible, paginée avec sommaire et facilement exploitable.	Départageant	/15
TOTAL (NOTE_TECH)			**/80**

On notera : $\mathbf{AD\_TECH} = \mathbf{NOTE\_AD} + \boldsymbol{NOTE\_TECH}$

N.B : Seuls les soumissionnaires dont la somme des notes administratives ($NOTE\_AD$) et techniques ($NOTE\_TECH$) est supérieure ou égale à 70 seront éligibles à l'analyse financière.

La condition d'éligibilité à l'analyse financière est donc : $AD\_TECH \geq 70$

ANALYSES FINANCIERE

La méthode utilisée dans ce cas de figure est celle du moins disant. Il s'entend comme le coût le plus bas proposé pour une formation par le soumissionnaire éligible à l'analyse financière.

On notera **:**

$\boldsymbol{MONT\_FIN_i}$ le montant proposé par le prestataire éligible pour la formation $\boldsymbol{i}$.

$\boldsymbol{NP_i}$ la note finale du prestataire pour la formation $\boldsymbol{i}$

$$NP_i = \frac{MONT\_FIN_i}{AD\_TECH_i}$$

Le prestataire retenu pour la formation i (PR_i) sera celui ayant le NP_i le plus bas.

ANNEXES

LETTRE DE SOUMISSION

SOUMISSION (MODELE ENTREPRISES)

Je soussigné (e) (nom ; prénom et fonction)

……,

Agissant en vertu des pouvoirs, a moi conférés, au nom et pour le compte de l'entreprise (la société)

……..

- *Siege social*
  ……..
- *Registre du commerce*
  ……
- *Forme juridique*
  ……
- *Numéro de compte contribuable*
  ……..
- *Numéro d'immatriculation*
  ……..
- *Numéro d'agrément de fonctionnement*
  ……..
- *Et faisant élection de domicile a*
  ……..

ENTREPRENEUR (EUSE)

Après m'être personnellement rendu (e) compte de la situation des lieux et après avoir apprécié, sous ma responsabilité, la nature et la difficulté du marché à exécuter,

Je me soumets et m'engage envers la BOAD à exécuter le marché, conforment aux conditions définies dans le cahier des charges, pour le cout global, défini par moi-même :

En chiffre ……..Francs CFA

En lettre

……..

Francs CFA toutes taxes comprises.

Les versements des sommes dues seront effectués par virement ou par chèque :

Au compte
№……..

Ouvert au nom de la société
……..……..

A la banque
……..
Située à ……..

J'affirme, sous peine de résiliation, de plein droit ou de mise en règle aux torts exclusifs de la société pour laquelle j'interviens que ladite société ne tombe pas sous le coup d'interdictions légales éditées, soit en au Togo, soit dans l'Etat ou siège la société.

Fait (ville) ……., le ……/…/…….

MODÈLE DE PRESENTATION DES OFFRES TECHNIQUES

- L'intitulé de la formation ;
- La présentation de la formation ;
- Les objectifs pédagogiques ;
- Les résultats attendus ;
- Les prérequis au cas échéant ;
- La population cible ;
- Le contenu de la formation
- Les moyens et méthodes andragogiques ;
- Les modalités d'évaluation des acquis ;
- Les outils didactiques ;
- La durée en volume horaire et en jour de la formation ;
- Les qualifications des formateurs et leur expérience par thème choisi ;
- Les références de l'organisme de formation ou son expérience dans le domaine de la formation continue notamment en ce qui concerne le thème choisi ;
- Le cout total ;
- Le lieu de formation
- Le nom du formateur :
- Les qualifications, certifications et références du formateur :

MODELE DE PRESENTATION DE L'OFFRE FINANCIERE

- Thème de formation ;
- Effectif ;
- Nombre de groupe ;
- Effectif par groupe ;
- Durée de la formation (5 jours maximum pour des formations spécifiques pouvant être sensiblement allongée si dûment justifiée.);
- Volume horaire total par groupe (40 heures maximum pour des formations spécifiques pouvant être sensiblement allongée si dûment justifiée.) ;

DESIGNATION	NOMBRE DE PARTICIPANTS	PRIX UNITAIRE	PRIX DE GROUPE	PRIX TOTAL
Conception du cours				
Diffusion (Horaires du formateur)				

Support pédagogique				
Autres documents				
Attestation de stage				
Pause - Café				
Repas (A ne pas facturer)				
Location de salle				
Cocktail				
Transport (éventuellement)				
Autre (préciser)				
Marge commerciale				
TOTAL GENERAL HT				
REMISE (EVENTUELLEMENT)				
TOTAL GENERAL A PAYER				

N.B : Remplir les cases si cela est nécessaire (EX : ne remplissez pas la ligne location de salle si vous n'en louez pas).

DETERMINATION DU COUT PAR PARTICIPANT

COUT TOTAL (1)	**VOLUME HORAIRE TOTAL**	**NOMBRE DE PARTICIPANT (2)**	**PRIX PAR PARTICIPANT = (1) / (2)**