ACCORD CADRE A BONS DE COMMANDES

N°2024_AOO_PRESTACYB

Cahier des Clauses Techniques Particulières (CCTP)

« PRESTATIONS D'ASSISTANCE A MAITRISE D'OUVRAGE ET FORMATIONS LIEES A LA SECURITE DES SYSTEMES D'INFORMATIONS »

Procédure de passation :

Appel d'offres ouvert en application des articles L2124-2, R2124-2 et R2161-2 à R2161-5 du code de la commande publique.

Table des matières

Définitions :

Les termes ci-dessous définis auront entre les Parties la signification suivante :

- « **Accord-Cadre** » désigne le présent accord-cadre à bons de commande notifié par la CANUT au Titulaire, étant précisé que chaque Lot donne lieu à l'attribution d'un Accord-Cadre.
- « **AE** » désigne l'acte d'engagement.
- « **Bénéficiaires** » désigne les Membres qui peuvent bénéficier de l'Accord-Cadre.
- « **BPU** » désigne le bordereau de prix unitaires.
- « **CCAG-TIC** » désigne le cahier des clauses administratives générales applicables aux marchés publics de techniques de l'information et de la communication (TIC).
- « **CCAP** » désigne le présent cahier des clauses administratives particulières.
- « **CCTP** » désigne le cahier des clauses techniques particulières de l'Accord-cadre.
- « **CMDB** » désigne la base de données de gestion des configurations du système d'information
- « **Lot** » : désigne chaque lot de l'Accord-Cadre.
- « **Membres** » désigne les adhérents, membres et partenaires de la CANUT.
- « **Notification** » désigne l'action consistant à porter une information ou une décision à la connaissance de la ou des Parties par tout moyen matériel ou dématérialisé permettant de déterminer de façon certaine la date de sa réception. La date de réception, qui peut être mentionnée sur un récépissé, est considérée comme la date de la Notification.
- « **OSCP** » (Offensive Security Certified Professional) est une certification technique qui atteste de compétences pratiques en tests d'intrusion et en hacking éthique
- « **Parties** » désigne la CANUT et le Titulaire.
- « **Titulaire** » désigne l'opérateur économique auquel a été attribué l'Accord-Cadre ou un de ses lots. En cas de groupement des opérateurs économiques, le titulaire désigne les membres du groupement, représenté, le cas échéant, par son mandataire.

Article 1 Pouvoir adjudicateur

Le pouvoir adjudicateur contractant est la CANUT, association Loi 1901, SIRET 92443595100018.

La CANUT intervient pour le compte de ses membres, collectivités territoriales, agences et établissements intervenant dans le secteur des secours, établissements d'enseignement publics, établissements publics intervenant dans le secteur de la recherche, établissements publics administratifs, syndicats mixtes, établissements publics de coopération intercommunale, sociétés publiques locales, groupements d'intérêt publics, régies, associations syndicales autorisées, établissements publics à caractère industriel et commercial.

La CANUT est un pouvoir adjudicateur passant des accords-cadres destinés à ses membres, qui sont des acheteurs au sens des articles L2113-2 à L2113-5 du code de la commande publique.

Adresse : 4 place Amédée Bonnet 69002 Lyon.

Représentant du pouvoir adjudicateur : le président de la CANUT.

Adresse de publication des consultations de la CANUT : https://www.marches-publics.info/

Pour tout renseignement sur le dossier de consultation : canut@canut.org

Article 2 Objet

La présente consultation a pour objet l'attribution par la CANUT, agissant en tant que centrale d'achats sur le fondement des dispositions de l'article L. 2113-2 du Code de la Commande Publique, d'un Accord-Cadre portant sur :

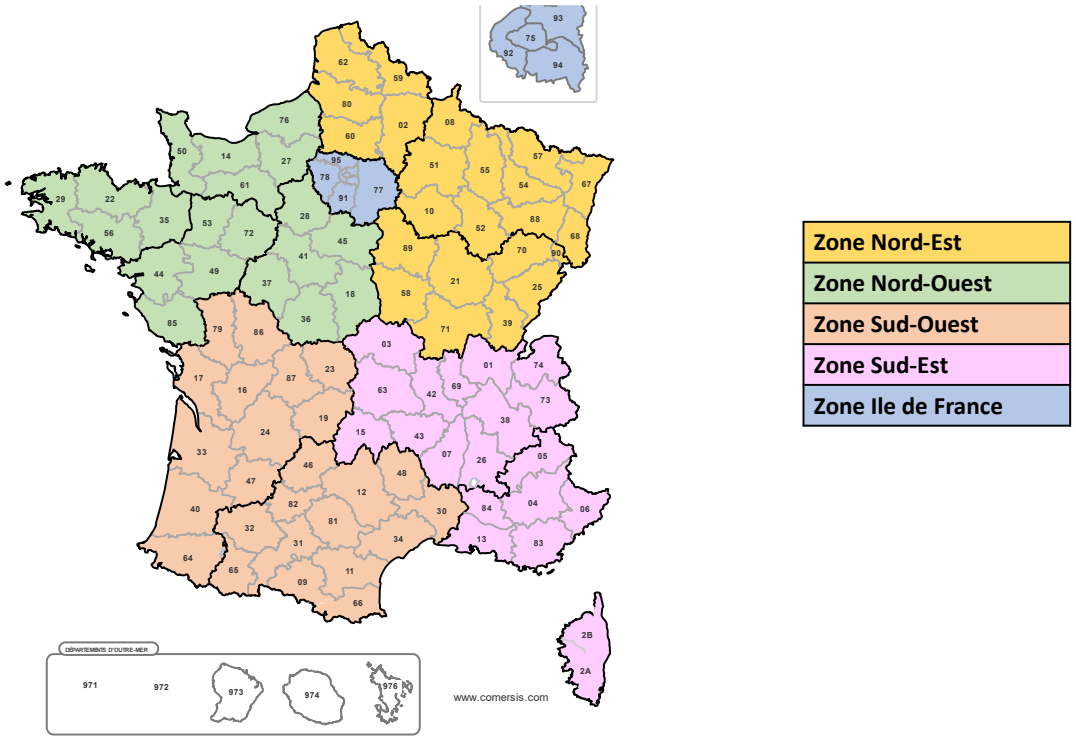
La mise à disposition de prestations intellectuelles et de tarifs journaliers (lots 1 à 6) permettant l'accompagnement de ses bénéficiaires dans la sécurisation de leurs systèmes d'information. Ces prestations sont également complétées (lot 7) par un ensemble de formations techniques et organisationnelles de haut niveau permettant aux Directions des Systèmes d'Information, aux RSSI et aux Maitrises d'Ouvrage d'obtenir des parcours pédagogiques certifiant autour de la cybersécurité.

Article 3 Allotissement

L'accord-cadre comporte 7 lots :

- LOT 1 : Prestations liées à la Sécurité des Systèmes d'Information sur l'ensemble du territoire métropolitain et DROM-COM
- LOT 2 : Prestations liées à la Sécurité des Systèmes d'Information en Zone Ile De France
  - La zone Ile de France comprend les départements 75, 77, 78, 91, 92, 93, 94, 95
- LOT 3 : Prestations liées à la Sécurité des Systèmes d'Information en Zone Nord-Ouest
  - La zone nord-ouest comprend les régions et départements suivants :
    - Bretagne : 22, 29, 35, 56
    - Centre Val de Loire : 18, 28, 36, 37, 41, 45
    - Normandie : 14, 27, 50, 61, 76
    - Pays de la Loire : 44, 49, 53, 72, 85
- Lot 4 : Prestations liées à la Sécurité des Systèmes d'Information en Zone Nord-Est
  - La zone nord-est comprend les régions et départements suivants :
    - Haut de France : 02 ,59 ,60 ,62 ,80
    - Grand Est : 08, 10 ,51 ,52 ,54 ,55 ,57 ,67 ,68 ,88
    - Bourgogne-Franche Comté : 21, 25, 39, 58, 70, 71, 89, 90

- Lot 5 : Prestations liées à la Sécurité des Systèmes d'Information en Zone Sud-Ouest
    - La zone sud-ouest comprend les régions et départements suivants :
    - Nouvelle-Aquitaine : 16, 17, 19, 23, 24, 33, 40, 47, 64, 79, 86, 87
    - Occitanie : 09, 11, 12, 30, 31, 32, 34, 46, 48, 65, 66, 81, 82
- Lot 6 : Prestations liées à la Sécurité des Systèmes d'Information en Zone Sud-Est
    - La zone sud-est comprend les régions et départements suivants :
        - Auvergne-Rhône-Alpes : 01, 03, 07, 15, 26, 38, 42, 43, 63, 69, 73, 74
        - Corse : 2A, 2B
        - Provence-Alpes-Côte d'Azur : 04, 05, 06, 13, 83, 84
- Lot 7 : Formations liées à la Sécurité des Systèmes d'Information sur l'ensemble du territoire métropolitain et DROM-COM



Article 4 Parties

L'Accord-Cadre est attribué par la CANUT en tant que pouvoir adjudicateur, pour le compte de ses membres. Les différentes parties pour l'exécution du contrat sont décrites dans les paragraphes suivants.

4.1 La CANUT

Elle est représentée par la personne en charge de piloter l'Accord-Cadre et/ou par un de ses dirigeants lors des réunions de pilotage.

Elle est responsable de toutes les questions administratives et des communications qui concernent l'Accord-Cadre entre le Titulaire et les Bénéficiaires. Les communications impliquant la CANUT doivent être soumises à sa validation avant tout envoi.

Elle est destinataire de tous les éléments de pilotage et des reportings périodiques exigés dans l'exécution de l'Accord-Cadre.

4.2 Le Bénéficiaire

Chaque établissement ou groupement souscrivant à l'Accord-Cadre par une convention de mise à disposition prend la qualité de Bénéficiaire (pour un groupement, l'ensemble de ses membres acquièrent cette qualité et sont identifiés pour le Titulaire).

Un Bénéficiaire peut avoir plusieurs points de contacts. Chaque Bénéficiaire doit être considéré comme un client à part entière et être pris en charge commercialement et techniquement par le Titulaire.

Le Bénéficiaire exécute l'Accord-Cadre directement auprès du Titulaire (demande de devis, commandes, paiements). Il peut appliquer les pénalités prévues dans l'Accord-Cadre si nécessaire.

Les Bénéficiaires sont des établissements implantés en France métropolitaine, et dans les DROM-COM.

4.3 Le Titulaire

Le Titulaire prend en charge la livraison des produits et prestations décrits dans le CCTP et dans son offre conformément aux dispositions de l'Accord-Cadre. Il est responsable du respect des engagements décrits dans l'Accord-Cadre auprès des Bénéficiaires et de la CANUT.

Il s'assure avant d'exécuter ses prestations auprès d'un établissement, que ce dernier a bien la qualité de Bénéficiaire.

Article 5 Description du besoin

5.1 Environnement / situation actuelle

Les collectivités territoriales (CT) sont engagées dans une transformation numérique profonde, autant pour répondre à des obligations règlementaires qu'à un souci de rendre un meilleur service aux citoyens.

Cette dépendance de plus en plus forte aux systèmes d'information (SI), couplée à l'hétérogénéité dans la taille et dans les moyens des collectivités, crée une fragilité. Au même titre que les SI de l'État, des opérateurs d'importance vitale (OIV) ou des opérateurs de services essentiels (OSE), la protection des SI des collectivités territoriales fait partie des champs prioritaires définis par la revue stratégique de cyberdéfense (RSC) de 2018, pour consolider le modèle national de cyberdéfense.

Au-delà de l'application de mesures, qu'elles soient d'hygiène ou techniques, de gouvernance, organisationnelles et humaines, la dimension règlementaire et juridique est essentielle pour assurer une meilleure prise en compte des risques numériques.

Dans ce contexte les bénéficiaires de la CANUT doivent pouvoir s'appuyer sur des tiers de confiance pour :

- Bénéficier de formations valorisantes en cybersécurité,
- Être accompagnés dans la transformation et la sécurisation de leurs systèmes d'information.

Le présent Accord-Cadre répond à plusieurs besoins prédéfinis.

Le candidat devra répondre à tous les besoins exprimés.

5.2 Objectifs

Cette consultation a pour objectif(s) de mettre à disposition des Bénéficiaires de la CANUT :

- Un ensemble de prestations (**lot 1 à 6**) pouvant être regroupées selon les thématiques suivantes :
  - Prestations de stratégie et de pilotage, en structurant la démarche pour répondre aux exigences règlementaires,
  - Prestation de pilotage global de la sécurité du système d'information pouvant aller jusqu'à la mise en œuvre d'un Système de Management de la Sécurité du Système d'Information (SSI).
  - Audits, contrôles et connaissance du risque :

- Audits nécessaires pour connaître son niveau de sécurité et élaborer des feuilles de route concrètes,
- Contrôle d'homologation de la SSI de l'établissement à la loi, aux règlements, aux normes qualités,
- Accompagnement dans l'analyse de risque, incluant les analyses de risques métiers,
- Réalisation de tests d'intrusion à l'occasion d'un changement d'un pan du système d'information.

➢ Intégration de la sécurité dans les projets,

❖ Un ensemble de formations (**lot 7**) techniques et organisationnelles de haut niveau permettant aux Directions des Systèmes d'Information, aux RSSI et aux Maitrises d'Ouvrage d'obtenir des parcours pédagogiques certifiants.

5.1 LOT 1 : Prestations liées à la Sécurité des Systèmes d'Information sur l'ensemble du territoire métropolitain et DROM-COM

5.1.1 Exigences métiers et techniques attendues

5.1.1.1 Exigences techniques

➢ Le candidat doit présenter une réelle expérience et expertise avec les collectivités territoriales afin de répondre pleinement aux attentes des bénéficiaires de la CANUT,

➢ Le candidat doit présenter une réelle expérience et expertise sur les différents périmètres couverts dans le cadre de la présente consultation,

➢ Le candidat devra figurer dans la liste des prestataires d'accompagnement et de conseil en sécurité des systèmes d'information (PACS) qualifiés ou en cours de qualification de l'Agence Nationale de la Sécurité des Système d'Information

- **Cette exigence ne porte que sur l'activité « Conseil en préparation à la gestion de crise d'origine cyber » du référentiel PACS de l'ANSSI.**
- **La qualification PACS étant relativement récente, les activités en cours de qualification seront considérées comme recevables, sur justificatif. Le candidat doit fournir le justificatif officiel de l'ANSSI prouvant que sur cette activité, il en est au stade J1 de la procédure.**

➢ Le candidat devra figurer dans la liste des prestataires d'audit de la sécurité des systèmes d'information (PASSI) qualifiés de l'Agence Nationale de la Sécurité des Système d'Information :

- Le candidat devra posséder et justifier les visas de sécurité PASSI RGS de l'ANSSI sur les 5 niveaux d'activité leur permettant de réaliser les missions suivantes inscrites au BPU :

PCY_L1_PASSI_ARCHI	Prestation auditeur PASSI - Audit d'architecture
PCY_L1_PASSI_CONF	Prestation auditeur PASSI - Audit de configuration
PCY_L1_PASSI_CODE	Prestation auditeur PASSI - Audit de code
PCY_L1_PASSI_PENT	Prestation auditeur PASSI - Test d'intrusion
PCY_L1_PASSI_ORGA	Prestation auditeur PASSI - audit organisationnel et physique

Remarque : la qualification PASSI datant de 2018, les activités en cours de qualification ne seront pas considérées comme recevables.

5.1.1.2 Exigences règlementaires et légales

L'offre du soumissionnaire doit en tout point respecter le cadre règlementaire, le cadre normatif et le cadre légal qui organise la politique de sécurité des bénéficiaires de la CANUT.

Les principaux textes de références sont les suivants :

- Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2)
- Certification des Hébergeurs de Données de Santé,
- Le Référentiel Général de Sécurité (RGS),
- Le Règlement no 910/2014 dit « eidaS »
- La loi de Programmation Militaire (LPM),
- La loi pour une République numérique (LRN),
- Le Référentiel Général d'Interopérabilité (R.G.I),
- ISO 27001 « système de gestion de la sécurité des systèmes d'information »,
- ISO 20000 « système de gestion de la qualité des services »,
- Règlement Général à la Protection des Données (RGPD),
- Recommandations du guide des 42 mesures d'hygiène de l'ANSSI.

5.1.2 Moyens, organisation, compétences attendues

- Le candidat doit présenter :
  - Son organisation détaillée permettant de satisfaire les besoins et objectifs de l'Accord-Cadre ;
  - Le nombre de missions et le chiffre d'affaires réalisés sur le lot considéré en 2023 ;
  - Les expertises et certifications des intervenants ; le candidat devra présenter des profils certifiés OSPC
  - Afin d'illustrer son expertise, le candidat **fournira 5 références significatives** réalisées auprès d'établissements publics (collectivités, bailleurs sociaux, établissements d'enseignement), sur une période récente (2022-2023), et correspondant au périmètre géographique du lot 1.

5.1.3 Maillage territorial et moyens humains

- Les prestations peuvent s'effectuer à distance, mais nécessitent également des rendez-vous physiques et des interventions sur les sites des bénéficiaires de la CANUT.
- Dans le cadre du lot 1, il est donc attendu un bon maillage sur le territoire hexagonal et ultra-marin permettant d'offrir cette proximité.
- L'ensemble du territoire doit être couvert, le candidat présentera la répartition de ses sites géographiques, le nombre de personnes et le type de profils.
  - Pour le profil « junior » : ayant moins de 3 ans d'expérience dans le domaine de la sécurité des systèmes d'information,
  - Pour le profil « sénior » ayant de 3 à 7 années d'expérience dans le domaine de la sécurité des systèmes d'information
  - Pour le profil « expert », » ayant plus de 7 années d'expérience dans le domaine de la sécurité des systèmes d'information
  - Pour le profil RSSI Mutualisé, ayant plus de 5 ans d'expérience minimum en tant que RSSI ou Profil P3 expert
- Le candidat indiquera, pour chaque catégorie, le nombre de profils dont il dispose. Un tableau synthétique doit être fourni à l'appui de cette demande. Il **peut** revêtir la forme suivante

Type de profil*	Nombre de profils disponibles pour le marché
Effectifs en capacité de réaliser les prestations	
Profil P1 Junior	
Profil P2 Senior	
Profil P3 Expert	
Auditeur PASSI - Audit d'architecture	
Auditeur PASSI - Audit de configuration	
Auditeur PASSI - Audit de code	
Auditeur PASSI - Test d'intrusion	
Auditeur PASSI - Audit organisationnel et physique	
RSSI Mutualisé	
Profils certifiés OSPC	

***Les CV correspondants devront être fournis dans une CVthèque organisée et indexée pour justifier des nombres indiqués. La CVthèque devra être annexée au mémoire technique**

5.1.4 Prestations attendues

Le périmètre des prestations couvre l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à garantir la sécurité du patrimoine informationnel du bénéficiaire et des processus métiers qui y sont liés, et plus particulièrement sur les domaines :

- ✓ Du système d'information du bénéficiaire
- ✓ Des infrastructures informatiques et de communication ;
- ✓ Des systèmes d'information d'ingénierie civile et de sécurité des bâtiments ;
- ✓ De la sécurité des biens et des personnes
- ✓ De la gestion des risques des systèmes d'information.

Les services proposés peuvent être regroupés autour de plusieurs pôles de prestations

5.1.4.1 Fourniture de prestations de gouvernance et de stratégie en matière de sécurité

Ces prestations peuvent être : (liste non exhaustive)

- ➢ La structuration de la sécurité à travers un accompagnement spécifique,
- ➢ La mise en œuvre de la politique de sécurité,
- ➢ L'intégration de la sécurité dans les projets,
- ➢ La constitution de modalités de pilotage de la sécurité des SI (tableaux de bord, suivi d'audit…),
- ➢ La mise en place de gestion de crise,

- L'analyse et la gestion des risques,
- L'audit,
- La conformité méthodologique et normative (ISO 27 799 et évolutions, NIS 2, …),
- La définition des bonnes pratiques (ITIL…),
- La définition des niveaux de services de sécurité (SLA…),
- Tout processus en lien avec la Sécurité des Systèmes d'Information
- …

Les devis exprimés pour répondre aux besoins en matière d'organisation et de management de la sécurité s'appuieront sur les profils SSI juniors, experts et confirmés et /ou des profils PASSI adéquats.

5.1.4.2 Prestations techniques de sécurité

L'offre proposée permet d'adresser en particulier les besoins suivants (liste non exhaustive) :

- Conseil en architecture,
- Assistance dans la définition des règles techniques de sécurité et dans la mise en œuvre des déclinaisons opérationnelles,
- Définition et mise en place des consignes et outils de gestion opérationnelle de la sécurité logique (socles de sécurité, gestion des mots de passe, des antivirus, des accès externes, cloisonnement du SI) et physique,
- Formalisation des procédures opérationnelles pour l'ensemble des systèmes et applications,
- Assistance à la définition et mise en place de socles de sécurité (Sécurité OS, BDD, virtualisation, réseaux, télécommunications…),
- Assistance / qualification des nouvelles vulnérabilités (Patchs applicatifs, systèmes...),
- Assistance à la désinfection de postes contaminés par des malwares,
- Tests d'intrusions (externe, interne, application web, WIFI…),
- Etat de l'art et transferts de compétences sur certaines technologies ou vulnérabilités et risques associés,
- …

Les devis exprimés pour répondre aux besoins en matière d'organisation et de management de la sécurité s'appuieront sur les profils SSI juniors, experts et confirmés et /ou des profils PASSI adéquats.

5.1.4.3 Monitorat et assistance technique

L'objet est notamment (liste non exhaustive) de :

- Comparer financièrement et techniquement des scénarios, des options ou des alternatives,
- Aider à la mise en œuvre de maquettes permettant d'évaluer et de comparer des solutions (avec si nécessaire des prêts de matériels),
- Réaliser des démonstrateurs permettant de juger de la pertinence d'un choix,
- Réaliser des transferts de compétences sur de nouvelles technologies adoptées,
- Présenter l'état de l'art sur un domaine technique donné,
- Proposer des procédures organisationnelles (au sein des équipes des bénéficiaire) accompagnant les évolutions,
- …

Les devis exprimés pour répondre aux besoins en matière d'organisation et de management de la sécurité s'appuieront sur les profils SSI juniors, experts et confirmés et /ou des profils PASSI adéquats.

5.1.4.4 Exercices de crise CYBER

La réalisation d'exercices de crise cybersécurité au sein des bénéficiaires de la CANUT n'est pas rendu actuellement obligatoire par les textes et la législation.

L'avènement de la directive NIS 2 et sa transposition dans la législation française peut changer la donne.

Néanmoins, l'Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI) met à disposition des collectivités territoriales un kit d'exercice de crise disponible sur son site Le kit d'exercice pour les collectivités territoriales | ANSSI

Sur cette base, la présente consultation propose des prestations forfaitisées dont le but est de sensibiliser et préparer tous les acteurs du secteur (élus, directions, métiers, DSI, etc.) aux risques cybersécurité dans leurs contextes particuliers.

- Le candidat doit prendre en compte dans sa réponse que ses intervenants devront obligatoirement être sur place.
- Pour cette prestation, il est attendu a minima 2 profils de type senior et/ou expert
- Le candidat devra indiquer un coût forfaitaire répondant à la réalisation d'une simulation de crise « standard » ainsi qu'une simulation de crise conforme au référentiel « PACS » dont le contenu devra a minima respecter les étapes, contenus et livrables suivants :
  - ✓ **Phase de cadrage**
    - Cette phase a pour objectif de cadrer le projet et d'en prendre en compte le contexte et les objectifs :
      - Définir les objectifs de la mission
      - Planification :
        - D'une réunion de lancement d'une heure (partage des objectifs, durée et format de l'exercice, définition de la logistique)
        - D'une date pour l'exercice
      - Identification du contexte
      - Définir l'organisation de gestion de crise, les participants à l'exercice, leur contact, leur fonction et leur rôle au sein de la cellule
    - Livrables obligatoires :
      - Compte-rendu ou note de lancement
      - Document de logistique nécessaire à fournir
      - Annuaire des participants complété
      - Fourniture du kit d'exercice « SIMULATION » pour les collectivités territoriales de l'ANSSI,
      - Création d'une boîte mail spécifique à l'exercice.
  - ✓ **Phase d'Animation**
    - Briefer l'ensemble des participants à l'exercice de crise
    - Pilotage de l'exercice de crise et mise en situation de la cellule de crise,
    - Evaluer le dispositif, étude des réactions par un observateur central,
    - Lancement des stimuli, réponses aux sollicitations de la cellule de crise, ...
    - Cette phase se termine par un débriefing à chaud
    - Livrables :
      - Brief des participants
      - Chronogramme
      - Stimuli Collectivité
      - Debriefing de l'exercice de crise complété
  - ✓ **Phase de Restitution**
    - Préparer le retour d'expérience sur la base du questionnaire et des observations
    - Restituer l'exercice
    - Livrables :
      - Questionnaire de satisfaction envoyé et complété
      - Grille d'évaluation exercice de crise cyber complétée
      - Support de restitution
      - Préconisations

Remarque : il sera possible de compléter le dispositif à l'aide de journées complémentaires (unités d'œuvre au BPU : PCY_L1_CYBERCRISE_DAY ou PCY_L1_PACS_CYBERCRISE_DAY) dans les cas où le bénéficiaire souhaiterait un exercice sur mesure.

Remarque : les étapes décrites proposent un phasage qui peut différer de celui du candidat, néanmoins le contenu du présent cahier des charges doit se retrouver dans la réponse du candidat.

- **Dans sa réponse, le candidat décrira l'organisation mise en place pour répondre à ce besoin,**
- **Dans sa réponse, le candidat indiquera clairement le nombre d'intervenants qu'il prévoit pour répondre au besoin exprimé, ainsi que leurs profils tel qu'exprimés au bordereau de prix.**
- **Dans sa réponse le candidat décrira avec détail son savoir-faire en matière d'exercices de crise en détaillant 5 expériences significatives d'exercice de crise qu'il a réalisé.**

5.1.4.5 Prestation de RSSI mutualisé

L'objectif de la prestation est de favoriser la mutualisation du RSSI entre les bénéficiaires de la CANUT.
La prestation est prise en charge par un bénéficiaire puis répartie entre toutes les structures qui lui sont affiliées.
Idéalement, le bénéficiaire est un groupement
Les missions qui incombent au RSSI mutualisé sont variées (liste non exhaustive) :

- ✓ Diagnostics de la maturité de la SSI
- ✓ Cartographie du système d'information
- ✓ Diagnostics des équipements de sécurité
- ✓ Revue des règles de pare-feu
- ✓ Diagnostic de l'Active Directory, de la messagerie,
- ✓ Aide à l'élaboration du plan de sauvegarde, tests de restauration,
- ✓ …

L'approche se fera sous forme d'Assistance Technique en engagement de moyens et au tarif journalier, avec facturation au bénéficiaire ou directement aux structures bénéficiaires du service.

La prestation doit être réalisée par les profils RSSI mutualisé ou P3 expert prévu au BPU.

La prestation d'initialisation (Unité d'œuvre « PCY_L1_INIT_RSSI_SHARE » au BPU) comprend :

- Lancement : rencontre des interlocuteurs, présentation générale de la prestation (Périmètre référentiels utilisés, prérequis et données d'entrées nécessaires au déroulement de la prestation)
- Etat des lieux de l'existant
- Définition du périmètre d'intervention et de responsabilité avec le bénéficiaire qui paye la prestation et les ceux qui en bénéficieront
- Validation du tarif journalier et de la méthodologie de facturation (facturation au commanditaire) ou à chaque bénéficiaire)
- Feuille de route organisation et méthodologie proposées (livrables, planning prévisionnel)

La mutualisation comprend :

- Interventions basées sur une fréquence de jours par mois pour chaque bénéficiaire validé en phase d'initialisation, au TJ
- Gouvernance avec comités animés par le titulaire

Remarque : le périmètre d'établissements mutualisés peut évoluer en cours d'exécution de la prestation. Le titulaire pourra réajuster sa proposition en la faisant valider par ses interlocuteurs initiaux.

5.2 LOT 2 à 6 : Prestations liées à la Sécurité des Systèmes d'Information en région

5.2.1 Exigences métiers et techniques attendues

5.2.1.1 Exigences techniques

- Le candidat doit présenter une réelle expérience et expertise avec les collectivités territoriales afin de répondre pleinement aux attentes des bénéficiaires de la CANUT,
- Le candidat doit présenter une réelle expérience et expertise sur les différents périmètres couverts dans le cadre de la présente consultation,
- Le candidat devra figurer dans la liste des prestataires d'audit de la sécurité des systèmes d'information (PASSI) qualifiés de l'Agence Nationale de la Sécurité des Système d'Information :
    - Le candidat devra posséder et justifier les visas de sécurité PASSI RGS de l'ANSSI sur les niveaux d'activité lui permettant de réaliser les missions suivantes inscrites au BPU :

PCY_L2_PASSI_CONF	Prestation auditeur PASSI - Audit de configuration
PCY_L2_PASSI_PENT	Prestation auditeur PASSI - Test d'intrusion
PCY_L2_PASSI_ORGA	Prestation auditeur PASSI - Audit organisationnel et physique

Remarque : la qualification PASSI datant de 2018, les activités en cours de qualification ne seront pas considérées comme recevables.

5.2.1.2 Exigences règlementaires et légales

L'offre du soumissionnaire doit en tout point respecter le cadre règlementaire, le cadre normatif et le cadre légal qui organise la politique de sécurité des bénéficiaires de la CANUT.

Les principaux textes de références sont les suivants :

- Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2)
- Certification des Hébergeurs de Données de Santé,
- Le Référentiel Général de Sécurité (RGS),
- Le Règlement no 910/2014 dit « eidaS »
- La loi de Programmation Militaire (LPM),
- La loi pour une République numérique (LRN),
- Le Référentiel Général d'Interopérabilité (R.G.I),
- ISO 27001 « système de gestion de la sécurité des systèmes d'information »,
- ISO 20000 « système de gestion de la qualité des services »,
- Règlement Général à la Protection des Données (RGPD),
- Recommandations du guide des 42 mesures d'hygiène de l'ANSSI.

5.2.2 Moyens, organisation, compétences attendues

- Le candidat doit présenter :
    - Son organisation détaillée permettant de satisfaire les besoins et objectifs de l'Accord-Cadre ;
    - Le nombre de missions et le chiffre d'affaires réalisés sur le lot considéré en 2023 ;
    - Les expertises et certifications des intervenants ;

- Afin d'illustrer son expertise, le candidat **fournira 3 références significatives (par lot régional auquel il candidate)** réalisées auprès d'établissements publics (collectivités, bailleurs sociaux, établissements d'enseignement), sur une période récente (2022-2023), et correspondant au périmètre géographique du lot sur lequel il présente son offre.

5.2.3 Maillage territorial et moyens humains

- Les prestations peuvent s'effectuer à distance, mais nécessitent également des rendez-vous physiques et des interventions sur les sites des bénéficiaires de la CANUT.
- Il est donc attendu un très bon maillage sur le territoire de chaque zone permettant d'offrir cette proximité de service pour les lots 2 à 6.
- Les délais d'intervention ou de déplacement pour se rendre sur site doivent être inférieurs à 2 heures en tout point de la région pour les lots 2 à 6.
- Le candidat présentera la répartition de ses sites géographiques, le nombre de personnes et le type de profils :
  - Pour le profil « junior » : ayant moins de 3 ans d'expérience dans le domaine de la sécurité des systèmes d'information,
  - Pour le profil « sénior » ayant de 3 à 7 années d'expérience dans le domaine de la sécurité des systèmes d'information
  - Pour le profil « expert », » ayant plus de 7 années d'expérience dans le domaine de la sécurité des systèmes d'information
  - Pour le profil RSSI Mutualisé, ayant plus de 5 ans d'expérience minimum en tant que RSSI ou Profil P3 expert

Un tableau synthétique qui décrit précisément le maillage régional ainsi que la répartition des profils doit être fourni à l'appui de cette demande. Il **peut** revêtir la forme suivante :

Zone xxx		
Effectifs en capacité de réaliser les prestations		
Nombre	Profils	Lieux des équipes dans la région
	Juniors	
	Séniors	
	Experts	
	Auditeur PASSI - Audit de configuration	
	Auditeur PASSI - Test d'intrusion	
	Auditeur PASSI - Audit organisationnel et physique	
	RSSI Mutualisé	
	Profils certifiés OSPC	

***Les CV correspondants devront fournis dans une CVthèque organisée et indexée pour justifier des nombres indiqués. La CVthèque devra être annexée au mémoire technique**

5.2.4 Prestations attendues

Le périmètre des prestations couvre l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à garantir la sécurité du patrimoine informationnel du bénéficiaire et des processus métiers qui y sont liés, et plus particulièrement sur les domaines :

- ✓ Du système d'information du bénéficiaire
- ✓ Des infrastructures informatiques et de communication ;
- ✓ Des systèmes d'information d'ingénierie civile et de sécurité des bâtiments ;
- ✓ De la sécurité des biens et des personnes
- ✓ De la gestion des risques des systèmes d'information.

Les services proposés peuvent être regroupés autour de plusieurs pôles de prestations.

5.2.4.1 Fourniture de prestations de gouvernance et de stratégie en matière de sécurité

Ces prestations peuvent être : (liste non exhaustive)

- ➢ La structuration de la sécurité à travers un accompagnement spécifique,
- ➢ La mise en œuvre de la politique de sécurité,
- ➢ L'intégration de la sécurité dans les projets,
- ➢ La constitution de modalités de pilotage de la sécurité des SI (tableaux de bord, suivi d'audit…),
- ➢ La mise en place de gestion de crise,
- ➢ L'analyse et la gestion des risques,
- ➢ L'audit,
- ➢ La conformité méthodologique et normative (ISO 27 799 et évolutions, NIS 2, …),
- ➢ La définition des bonnes pratiques (ITIL…),
- ➢ La définition des niveaux de services de sécurité (SLA…),
- ➢ Tout processus en lien avec la Sécurité des Systèmes d'Information
- ➢ …

Les devis exprimés pour répondre aux besoins en matière d'organisation et de management de la sécurité s'appuieront sur les profils SSI juniors, experts et confirmés et /ou des profils PASSI adéquats.

5.2.4.2 Prestations techniques de sécurité

L'offre proposée permet d'adresser en particulier les besoins suivants (liste non exhaustive) :

- ➢ Conseil en architecture,
- ➢ Assistance dans la définition des règles techniques de sécurité et dans la mise en œuvre des déclinaisons opérationnelles,
- ➢ Définition et mise en place des consignes et outils de gestion opérationnelle de la sécurité logique (socles de sécurité, gestion des mots de passe, des antivirus, des accès externes, cloisonnement du SI) et physique,
- ➢ Formalisation des procédures opérationnelles pour l'ensemble des systèmes et applications,
- ➢ Assistance à la définition et mise en place de socles de sécurité (Sécurité OS, BDD, virtualisation, réseaux, télécommunications…),
- ➢ Assistance / qualification des nouvelles vulnérabilités (Patchs applicatifs, systèmes...),
- ➢ Assistance à la désinfection de postes contaminés par des malwares,

- Tests d'intrusions (externe, interne, application web, WIFI…),
- Etat de l'art et transferts de compétences sur certaines technologies ou vulnérabilités et risques associés,
- …

Les devis exprimés pour répondre aux besoins en matière d'organisation et de management de la sécurité s'appuieront sur les profils SSI juniors, experts et confirmés et /ou des profils PASSI adéquats.

5.2.4.3 Monitorat et assistance technique

L'objet est notamment (liste non exhaustive) de :

- Comparer financièrement et techniquement des scénarios, des options ou des alternatives,
- Aider à la mise en œuvre de maquettes permettant d'évaluer et de comparer des solutions (avec si nécessaire des prêts de matériels),
- Réaliser des démonstrateurs permettant de juger de la pertinence d'un choix,
- Réaliser des transferts de compétences sur de nouvelles technologies adoptées,
- Présenter l'état de l'art sur un domaine technique donné,
- Proposer des procédures organisationnelles (au sein des équipes des bénéficiaires) accompagnant les évolutions,
- …

Les devis exprimés pour répondre aux besoins en matière d'organisation et de management de la sécurité s'appuieront sur les profils SSI juniors, experts et confirmés et /ou des profils PASSI adéquats.

5.2.4.4 Prestation d'audit d'écart de sécurité

L'objectif de la présente unité d'œuvre est de mesurer l'écart entre ce qui est mis en place sur le système d'information d'un bénéficiaire et les règles d'hygiène énoncées par l'ANSSI (https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique)

L'unité d'œuvre s'articulera autour des phases suivantes :

- Analyse de l'existant
  - > Entretiens avec remise des procédures et de la documentation.
- Identification des vulnérabilités des systèmes et outils actuels,
  - > Une attention particulière sera portée sur l'innocuité de ces tests vis-à-vis du SI testé.
- Identification des écarts avec les règles d'hygiène
- Définition du plan d'actions sur les axes organisationnel et technique.

Cet audit d'écart doit faire l'objet d'échanges contradictoires avec les personnels du bénéficiaire de façon que le plan d'actions proposé soit consensuel.

Dans le cadre de cette prestation, les exigences suivantes sont demandées :

- L'audit de l'existant demandé doit permettre de donner une bonne visibilité des écarts entre les règles d'hygiène de l'ANSSI et la situation du système d'information audité. Le rapport d'audit doit être considéré comme confidentiel, seules les personnes ayant le besoin d'en connaitre doivent pouvoir y accéder.
- Le plan d'actions proposé doit être présenté de façon synthétique en remplissant la feuille Excel jointe en annexe 24_AOO_PRESTACYB _AUDIT_ECART.xlsx :

En annexe de ce document, le bénéficiaire doit pouvoir trouver :

1. Un document de synthèse concernant l'organisation du programme d'audit
2. Pour chaque projet :
    a. Un planning détaillé intégrant les charges pour le bénéficiaire associées aux jalons projets doit être tenu à jour ;
    b. Un document d'architecture technique comprenant le détail des produits utilisés (types, nombre de licences) ;
    c. Un document d'exploitation permettant l'exploitation du système, sa sauvegarde, sa reprise sur incident, les numéros d'urgence à appeler en cas d'incident.

L'ensemble des prestations peuvent être fournies depuis les locaux du prestataire. L'organisation doit être précisée avant le démarrage des travaux.

Pour des raisons de sécurité et de confidentialité, les équipes du prestataire seront localisées en Europe tout comme les données.

L'unité d'œuvre est décomposée en 3 phases majeures :

(a) Phase d'initialisation

La phase d'initialisation doit permettre de réaliser les actions suivantes :

- ✓ Mise en place des processus organisationnels et techniques entre le Titulaire et le bénéficiaire.
- ✓ Mettre en place les moyens techniques pour assurer les échanges de données entre le Titulaire et le bénéficiaire (Lien réseau, outil de chiffrement, partage de secrets…).

L'objectif étant de capitaliser sur les éléments existants, il est impératif de les utiliser pour constituer le socle de base sur les parties organisationnelles, processus et techniques.

(b) Phase d'analyse

La phase d'analyse doit permettre de mesurer les écarts vis-à-vis des règles d'hygiène de l'ANSSI :

- ✓ Prise d'empreinte, cartographie de l'infrastructure, cartographie applicative :
  > Corrélation avec la CMDB existante.
- ✓ Scan de conformité et de vulnérabilités
- ✓ Définir le plan d'actions

- ❖ **Les soumissionnaires décriront l'ensemble des livrables qui seront produits à la phase d'analyse.**
- ❖ **Les soumissionnaires devront spécifier les prérequis techniques et organisationnels nécessaires pour garantir le succès de cette phase et l'obtention des premiers résultats pertinents rapidement.**

(c) Phase de restitution du plan d'actions

La phase de restitution du plan d'actions doit prévoir au minimum trois réunions :

1. Une réunion au niveau direction avec pour objectif la présentation du plan d'actions macroscopique au regard des risques couverts. Le support devra présenter les risques avant la mise en œuvre des actions et les risques couverts par chaque action.
2. Une réunion au niveau managérial avec pour objectif la présentation des mesures organisationnelles à mettre en œuvre. Ces mesures devront présenter les évolutions nécessaires dans le modèle d'organisation du bénéficiaire en déclinant par exemple les évolutions dans les processus existants et la description des tâches à insérer dans les fiches de postes des agents. Une fiche de synthèse des charges projets et récurrentes devra être présentée.
3. Une réunion au niveau techniques avec pour objectif la présentation des projets techniques à mener, présentés sur une échelle de temps réaliste. La présentation devra intégrer une fiche synthétique par projet (Objectifs, planning, principaux jalons, charge en jour/homme pour le personnel du bénéficiaire).

5.2.4.5 Exercices de crise CYBER

La réalisation d'exercices de crise cybersécurité au sein des bénéficiaires de la CANUT n'est pas rendu actuellement obligatoire par les textes et la législation.

L'avènement de la directive NIS 2 et sa transposition dans la législation française peut changer la donne.

Néanmoins, l'Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI) met à disposition un kit d'exercice de crise pour les collectivités disponible sur son site Le kit d'exercice pour les collectivités territoriales | ANSSI

Sur cette base, la présente consultation propose des prestations forfaitisées dont le but est de sensibiliser et préparer tous les acteurs du secteur (élus, directions, métiers, DSI, etc.) aux risques de cybersécurité dans leurs contextes particuliers.

- Le candidat doit prendre en compte dans sa réponse que ses intervenants devront obligatoirement être sur place.

  Le candidat devra indiquer un coût forfaitaire répondant à la réalisation d'une simulation de crise « standard » ainsi qu'une simulation de crise conforme au référentiel « PACS » dont le contenu devra à minima respecter les étapes, contenus et livrables suivants :

  - ✓ **Phase de cadrage**
    - Cette phase a pour objectif de cadrer le projet et d'en prendre en compte le contexte et les objectifs :
      - Définir les objectifs de la mission
      - Planification :
        - D'une réunion de lancement d'une heure (partage des objectifs, durée et format de l'exercice, définition de la logistique)
        - D'une date pour l'exercice
      - Identification du contexte
      - Définir l'organisation de gestion de crise, les participants à l'exercice, leur contact, leur fonction et leur rôle au sein de la cellule
    - Livrables obligatoires :
      - Compte-rendu ou note de lancement
      - Document de logistique nécessaire à fournir
      - Annuaire des participants complété
      - Fourniture du kit d'exercice « SIMULATION » pour les collectivités territoriales de l'ANSSI,
      - Création d'une boite mail spécifique à l'exercice.
  - ✓ **Phase d'Animation**
    - Briefer l'ensemble des participants à l'exercice de crise
    - Pilotage de l'exercice de crise et mise en situation de la cellule de crise,
    - Evaluer le dispositif, étude des réactions par un observateur central,
    - Lancement des stimuli, réponses aux sollicitations de la cellule de crise, ...
    - Cette phase se termine par un débriefing à chaud
    - Livrables :
      - Brief des participants
      - Chronogramme
      - Stimuli Collectivités
      - Debriefing de l'exercice de crise complété
  - ✓ **Phase de Restitution**
    - Préparer le retour d'expérience sur la base du questionnaire et des observations
    - Restituer l'exercice
    - Livrables :
      - Questionnaire de satisfaction envoyé et complété
      - Grille d'évaluation exercice de crise cyber complétée
      - Support de restitution
      - Préconisations

Remarque : il sera possible de compléter le dispositif à l'aide de journées complémentaires (unités d'œuvre au BPU : PCY_Lx_CYBERCRISE_DAY) dans les cas où le bénéficiaire souhaiterait un exercice sur mesure. (Lx correspond au numéro de lot)

Remarque : les étapes décrites proposent un phasage qui peut différer de celui du candidat, néanmoins le contenu du présent cahier des charges doit se retrouver dans la réponse du candidat.

- ❖ **Dans sa réponse, le candidat décrira sa méthodologie, depuis la prise de contact jusqu'à la restitution.**
- ❖ **Dans sa réponse, le candidat indiquera clairement le nombre d'intervenants qu'il prévoit pour répondre au besoin exprimés, ainsi que leur profil tel qu'exprimé au bordereau de prix.**

❖ **Dans sa réponse le candidat décrira avec détail son savoir-faire en matière d'exercices de crise en détaillant 5 expériences significatives d'exercice de crise débutant.**

5.2.4.6 Prestation de RSSI mutualisé

L'objectif de la prestation est de favoriser la mutualisation du RSSI entre les bénéficiaires de la CANUT.
La prestation est prise en charge par un bénéficiaire puis répartie entre toutes les structures qui lui sont affiliées.
Idéalement, le bénéficiaire est un groupement
Les missions qui incombent au RSSI mutualisé sont variées (liste non exhaustive) :

- ✓ Diagnostics de la maturité de la SSI
- ✓ Cartographie du système d'information
- ✓ Diagnostics des équipements de sécurité
- ✓ Revue des règles de pare-feu
- ✓ Diagnostic de l'Active Directory, de la messagerie,
- ✓ Aide à l'élaboration du plan de sauvegarde, tests de restauration,
- ✓ …

L'approche se fera sous forme d'Assistance Technique en engagement de moyens et au tarif journalier, avec facturation au bénéficiaire ou directement aux structures bénéficiaires du service

La prestation d'initialisation (Unité d'œuvre « PCY_Lx_INIT_RSSI_SHARE » au BPU (où Lx correspond au numéro du lot)) comprend :

- Lancement : rencontre des interlocuteurs, présentation générale de la prestation (Périmètre référentiels utilisés, prérequis et données d'entrées nécessaires au déroulement de la prestation)
- Etat des lieux de l'existant
- Définition du périmètre d'intervention et de responsabilité avec le bénéficiaire qui paye la prestation et les ceux qui en bénéficieront
- Validation du tarif journalier et de la méthodologie de facturation (facturation au commanditaire) ou à chaque bénéficiaire)
- Feuille de route organisation et méthodologie proposée (livrables, planning prévisionnel)

La mutualisation comprend

- Interventions basées sur une fréquence de jours par mois pour chaque bénéfciaire validé en phase d'initialisation, au TJ
- Gouvernance avec comités animés par le titulaire

Remarque : le périmètre d'établissements mutualisés peut évoluer en cours d'exécution de la prestation. Le titulaire pourra réajuster sa proposition en la faisant valider par ses interlocuteurs initiaux.

5.3 Lot 7 : Formations liées à la Sécurité des Systèmes d'Information sur l'ensemble du territoire métropolitain et DROM-COM

5.3.1 Objectif

Ce lot a pour objectif de mettre à disposition des bénéficiaires de la CANUT un catalogue complet de formations en matière de cybersécurité.

5.3.2 Périmètre technique

Le catalogue doit proposer des formations classiques et des formations certifiantes à minima sur les thématiques suivantes :

- Sécurité Offensive (Techniques de hacking, tests d'intrusion, OSINT, …)
- Sécurité Défensive (Investigations, sécurité applicative, matérielle, analyse de malware, sécurité du poste utilisateur, parcours analyste SOC, …)
- Gouvernance
- Normes et Méthodes (NIS 2, ISO xxxx, EBIOS RM, …)
- Juridique - RGPD et DPO
- Offre Éditeur (formations éditeurs et constructeurs ...)

Pour chaque thématique, il est attendu à minima un nombre de formations :

- Sécurité Offensive : 6 formations
- Sécurité Défensive : 15 formations
- Gouvernance : 6 formations
- Normes et Méthodes : 15 formations
- Juridique - RGPD et DPO : 3 formations
- Offre Éditeur (formations éditeurs et constructeurs ..) : 15 formations

Le non-respect de ces exigences quantitatives sera apprécié au regard du critère technique correspondant à la richesse du catalogue du candidat

En complément, le candidat pourra proposer l'ensemble des formations disponibles qui n'auraient pas été décrites. La profondeur du catalogue sera jugée.

Dans le cas de formations certifiantes, la prestation doit inclure une présentation à l'examen de certification. Un second passage à l'examen de certification pourra faire l'objet d'une facturation supplémentaire.

5.3.3 Exigences métiers et techniques attendues

Le candidat doit présenter :

- L'organisation de la société ou du groupement autour des prestations de formation permettant de satisfaire le besoin et les objectifs de l'Accord-Cadre ;
- Le chiffre d'affaires réalisés sur le lot considéré en 2023 ;
- Les expertises et certifications des intervenants ;
- Une réelle expérience et expertise dans le domaine de la formation liées à la cybersécurité afin de répondre pleinement aux attentes des bénéficiaires de la CANUT ;
- Sa certification QUALIOPI ;
- Le détail de l'ensemble des moyens pédagogiques, techniques, et logistiques mis à disposition des stagiaires ;
- Un catalogue de formation complet correspondant au périmètre technique spécifié au § 5.3.2.

5.3.4 Profils des formateurs

Tout animateur de formation doit :

- Être titulaire d'une certification valide correspondant à la nature du cours dispensé
- Avoir réalisé des missions concrètes utilisant les préceptes dispensés.

5.3.5 Plans et méthodes pédagogiques

Le candidat doit proposer 3 modes de formation, à savoir :

- Les formations « inter » dans ses locaux,
- Les formations « intra » dans les locaux du bénéficiaire,
- Les formations à distance.

Cette dernière doit permettre à un bénéficiaire de suivre la même formation qu'en présentiel tout en évitant des déplacements coûteux et en garantissant la performance et la sécurité des outils utilisés.

La durée type d'une journée de formation est de 7 heures (hors temps de pause du déjeuner).

Le bénéficiaire doit garder la possibilité de demander que les formations aient lieu hors périodes de vacances scolaires

(Zone académique correspondant au bénéficiaire).

Le candidat doit proposer des méthodes interactives permettant de prendre en compte et de corriger, le cas échéant, les connaissances des participants et leurs pratiques. L'offre de l'organisme proposera une partie théorique et une partie pratique (ceci constituera un des critères de sélection des offres).

5.3.5.1 Formations standards catalogue

- Le candidat doit proposer à minima dans son offre un catalogue de formation complet sur le périmètre technique spécifié au spécifié au § 5.3.2.
- Pour chaque formation, il doit être précisé si celle-ci donne lieu à une certification diplômante en fin de cursus.
- Le candidat doit également préciser la durée en jour(s) et doit préciser le nombre minimal de stagiaires pour que la formation ait bien lieu.

5.3.5.2 Formations non standards – formations spécifiques

- Le titulaire pourra être sollicité pour organiser et dispenser une formation spécifique à un besoin d'un bénéficiaire. Elle pourra être réalisée à façon en fonction des projets ou des profils inscrits.
- Le plan de formation peut être adapté par mixage des modules de différents programmes proposés en standard dans le catalogue en fonction des compétences spécifiques des stagiaires. Le tarif sera présenté sur la base d'un coût forfaitaire journalier pour un maximum de 10 stagiaires.

5.3.6 Matériel pédagogique

- Le candidat doit détailler l'ensemble des moyens pédagogiques, techniques, et logistiques mis à disposition des stagiaires.

5.4 Engagements de service

5.4.1 Compétences des intervenants

Chaque Bénéficiaire se réserve la possibilité de vérifier, au cours du déroulement des prestations, que les intervenants possèdent effectivement des compétences équivalentes à celles présentées lors de la phase d'avant-vente.

Elles seront également évaluées au regard du respect d'un certain nombre d'indicateurs tels que :

- La réalisation des prestations dans les délais fixés ;
- L'utilisation de méthodes et d'outils adaptés ;
- L'enrichissement des documentations ;
- La maîtrise des coûts ;
- La production de tableaux de bord et des plannings permettant le pilotage et le suivi d'activité (reporting).

Tout changement pendant une phase de projet devra faire l'objet d'une période de recouvrement d'une durée adaptée au contexte du projet.

Le Bénéficiaire pourra demander le remplacement d'un ou plusieurs intervenants par des personnels de compétences équivalentes durant l'exécution des prestations sans supplément de coût.

5.5 Plan d'assurance qualité

Le candidat doit fournir dans sa réponse un Plan d'Assurance Qualité détaillant les outils et méthodologies proposés pour assurer une qualité optimale dans l'exécution de l'Accord-Cadre pendant toute sa durée, auprès de la CANUT.

A destination des Bénéficiaires, un plan d'assurance qualité devra spécifiquement faire apparaitre la Politique de Sécurité des Systèmes d'Informations du Titulaire ainsi que les éventuels certificats de sécurité dont il dispose. Le Plan d'Assurance Qualité du titulaire devra faire apparaitre également la méthodologie d'intégration de la sécurité dans les projets du titulaire, les modalités de chiffrement des données, de traçabilité des actions ainsi que les dispositifs de protection des identités (méthode d'authentification et robustesse des secrets). Le titulaire devra être en mesure d'apporter des preuves documentées au Bénéficiaire attestant du respect de son assurance qualité.

5.6 Audit de sécurité

Le Bénéficiaire doit pouvoir, à tout moment, contrôler que les exigences de sécurité sont satisfaites par les dispositions prises par le Titulaire.

Les audits de sécurité concernent tous les équipements et personnels intervenant dans la gestion de l'infrastructure. Ils pourront avoir lieu au maximum une fois par an sur décision du Bénéficiaire.

Le contrôle peut s'effectuer selon les modalités suivantes sur place ou à distance :

- Visite des locaux du Titulaire avec entretiens individuels avec les membres de son équipe ;
- Accès aux machines impliquées dans l'administration de l'infrastructure ;
- Examen des différents registres et journaux (incidents de sécurité, visites des sociétés de maintenance, authentification des opérateurs) ;
- Identification des composants réseaux, systèmes, applicatifs du système d'information pouvant présenter une vulnérabilité ou une perméabilité ;
- Identification des personnels / services / prestataires pouvant présenter une vulnérabilité du fait de leur consigne de sécurité ou dans leur application de ces consignes ;
- Etude de ces vulnérabilités ou perméabilités afin d'en déterminer les prérequis d'exploitation et les impacts potentiels ;
- Exploitation de ces vulnérabilités ou perméabilités pour démontrer la possibilité effective d'obtenir des accès ou informations non accessibles dans le cas nominal d'utilisation ;
- Revue du code source des applications utilisées par le Bénéficiaire ;
- Revue de l'ensemble des accords de confidentialités qui concernent le Bénéficiaire.

Les audits pourront être réalisés par les équipes du Bénéficiaire ou délégués à un tiers non-concurrent direct ou indirect du Titulaire.

Cette visite est notifiée au Titulaire avec un délai minimal de préavis de 15 jours. L'ensemble des sites peut être concerné par une visite.

Le Titulaire facilitera l'accès des auditeurs aux zones d'hébergement, et assurera la disponibilité de son personnel pour la bonne conduite des audits. Les audits sont définis auparavant par une charte commune et par un plan d'audit qui sont validés et signés entre le Titulaire, l'exécutant de l'audit et le Bénéficiaire.

Les audits de sécurité pourront prendre la forme de tests d'intrusion techniques et organisationnels permettant de vérifier à la fois les infrastructures, les couches applicatives et le personnel de l'hébergeur.

Le titulaire détaillera dans sa réponse les éventuels frais qu'il appliquerait en cas de déclenchement de cette clause d'audit de sécurité.

5.7 Localisation et sauvegarde des données

Les lieux d'hébergement des données doivent satisfaire aux exigences de sécurité de la Personne Publique, aux dispositions de la loi du 6 janvier 1978 modifiée et au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Le Titulaire doit communiquer la liste de tous les lieux de stockage de données (site d'hébergement principal, site(s) de secours, etc.). Si la faisabilité technique de cette exigence est trop complexe, il peut être demandé au prestataire d'être en mesure de localiser, a posteriori, le lieu de stockage des données, en particulier pour donner suite à un incident.

Il sera également nécessaire de prévenir le Bénéficiaire en cas de modification des conditions du contrat amenant à transférer les données vers un datacenter hors de la France et en tout état de cause, aucune donnée ne sera stockée au repos hors du territoire de l'Union Européenne.

Le Titulaire doit communiquer sa politique de sauvegarde des données auprès des Bénéficiaires.

La sauvegarde doit rendre réutilisable l'ensemble des données, des médias et des configurations en cas de sinistre sur le site de production (notamment sinistre de type incendie et cyberattaque d'ampleur).

5.8 Direction de projet

L'importance de la direction du projet implique que la responsabilité globale de l'opération sera de la responsabilité du chef de projet du Titulaire.

Sa désignation nécessite l'accord du Bénéficiaire.

Le chef de projet aura en charge l'organisation et l'animation des comités du projet. Il mettra en place les outils nécessaires pour le suivi de projet

Le formalisme des documents produits devra être validé par le Bénéficiaire et devra être adapté en fonction des recommandations éventuelles de ce dernier.

5.9 Prestations réalisées par un groupement d'opérateurs

Dans le cas d'une prestation réalisée en groupement, le Titulaire présente de façon détaillée les relations techniques et fonctionnelles avec ses partenaires. Il fournit notamment :

- Les contrats le liant avec le ou les partenaires
- La description des projets communs opérationnels
- Les standards de communication utilisés
- Les outils d'administration communs/différents

Article 6 Généralités concernant l'exécution de l'Accord-Cadre

6.1.1 Emission des devis

Toute demande de devis devra être satisfaite dans un délai maximum de 10 jours ouvrés. Le délai court à réception de la demande de devis par mail.

En cas de non-respect du délai, des pénalités décrites dans l'annexe « Pénalités » pourront être appliquées par le Bénéficiaire.

6.1.2 Exigences de confidentialité et de propriété intellectuelle

Dans le cadre du présent accord-cadre, le bénéficiaire et le Titulaire conviennent qu'ils sont amenés à se transmettre et à recevoir des informations de nature confidentielle et/ou propriétaire. Le bénéficiaire et le titulaire acceptent de transmettre et de recevoir de telles informations dans les termes et conditions du présent accord-cadre.

Toute information ou document communiqué par le bénéficiaire au titulaire, sous quelque forme que ce soit, devra être considéré comme ayant un caractère confidentiel.

Toute donnée dont le titulaire a connaissance à l'occasion de l'exécution du présent accord-cadre est strictement couverte par le secret professionnel (article 226-13 du Code pénal).

Ne constituent pas des informations confidentielles les informations qui :

- Sont déjà connues du Titulaire qui les reçoit préalablement à la date de leur divulgation par le bénéficiaire et non soumises à des exigences de confidentialité.
- Sont disponibles dans le domaine public lors de leur divulgation ou tombent ultérieurement dans le domaine public, sans manquement aux stipulations de ce marché.
- Sont communiquées par un utilisateur de compte à privilège à titre non confidentiel au titulaire, dès lors que ce tiers n'est pas lié à l'autre partie par une quelconque obligation de confidentialité.
- Sont développées de manière indépendante par le titulaire qui les reçoit, en dehors de tout manquement aux stipulations de ce marché.

Le titulaire veille à ce qu'au cours de l'exécution du présent marché, soient respectées la sécurité et la confidentialité des données et des accès informatiques du bénéficiaire conformément aux lois et régimes applicables, et notamment conformément à la loi n° 78-17 du 6 janvier 1978 modifiée par la Loi du 6 août 2004 relative à l'informatique, aux fichiers et aux libertés, (article 29) et aux dispositions du code pénal en vigueur.

A ce titre, le titulaire s'engage :

- À n'utiliser les informations et documents délivrés par la Personne Publique qu'à sa demande exclusive et pour la finalité définie dans le présent marché.
- À ne pas divulguer à des tiers, à titre gratuit ou onéreux, et sous quelque forme que ce soit, les informations et documents communiqués par le bénéficiaire à l'occasion de l'exécution du présent marché.
- À prendre toutes les mesures pour que lesdites données ne puissent être accessibles à d'autres personnes que les personnels attachés à leur traitement et à leur analyse. Ces derniers seront sensibilisés au caractère stratégique des informations et documents confiés et liés au titulaire par un engagement de confidentialité.
- À ne pas procéder à des copies, utilisations ou diffusion de partie ou totalité d'un fichier et/ou d'une donnée détenue par le bénéficiaire ou installés sur une configuration, sur un support, sur un élément ou sur un sous-ensemble d'une configuration détenus par celle-ci, à l'exception des copies, utilisations ou diffusion nécessaires à l'exécution d'une prestation prévue au présent marché, auquel cas l'accord de la Personne Publique est nécessaire.
- À ne pas sortir du lieu d'hébergement des configurations, des supports numériques ou d'autres, d'éléments ou sous-ensembles d'une configuration, d'un matériel, ou d'une documentation détenue par le bénéficiaire sans l'autorisation préalable et écrite de celle-ci.
- En qualité de « sous-traitant du traitement » au sens de la loi n° 78-17 du 6 janvier 1978 en vigueur, à effectuer tout traitement de données personnelles dans le respect des lois et règlements applicables en matière de protection des données personnelles.

Le Titulaire sera responsable vis-à-vis du bénéficiaire de la perte de documents remis sous quelque forme que ce soit, ou de la divulgation volontaire ou involontaire d'informations communiquées. Le titulaire s'engage, à ce titre,

à aviser sans délai le bénéficiaire de toute disparition, ainsi que de tout incident ou suspicion d'incident pouvant révéler un risque de violation des présentes obligations.

Le présent marché prend effet à compter de sa notification et restera en vigueur jusqu'à la fin des prestations. Les parties resteront soumises aux obligations contenues dans le présent marché pendant une période de trois (3) ans suivant son expiration.

Le titulaire doit procéder à la destruction ou à la restitution de tous les fichiers manuels ou informatisés stockant les informations saisies, à l'échéance du présent marché ou sur ordre du bénéficiaire.

Les dispositions du présent article s'appliquant au titulaire s'appliquent également à tout opérateur économique intervenant pour le compte ou en partenariat avec le titulaire (cotraitants et sous-traitants notamment).

Sous réserve d'un préavis de quinze (15) jours ouvrés, le bénéficiaire se réserve le droit de procéder à toute vérification qui lui paraîtrait nécessaire pour constater le respect des obligations précitées par le titulaire. Il est toutefois entendu entre les parties qu'un tel audit ou toute autre forme de contrôle/ vérification ne peut en aucun cas porter sur les documents financiers et/ou comptables du Titulaire ou sur les documents relatifs aux membres du personnel du titulaire (sauf accord préalable et éclairé de ces derniers). En tout état de cause, le bénéficiaire reconnait que la conduite de toute forme d'audit est limitée à une fois par an. Le bénéficiaire s'engage à respecter les obligations de confidentialité qui lui incombent au titre des présentes ainsi que les règles d'accès et de sécurité en vigueur dans les locaux du titulaire et se porte fort du respect de ces règles par les membres de son personnel et/ou auditeur externe.

En cas de non-respect des dispositions précitées, la responsabilité du titulaire peut également être engagée sur la base des dispositions des articles 226-5 et 226-17 du code pénal.

Le bénéficiaire se réserve le droit d'exiger du titulaire du marché, sans versement d'aucune indemnité, le remplacement immédiat de tout agent salarié de l'entreprise qui aurait contrevenu aux règles précédemment édictées.

Le bénéficiaire pourra prononcer la résiliation immédiate du marché, sans indemnité en faveur du titulaire, en cas de violation du secret professionnel ou de non-respect des dispositions précitées.

Article 7 Reporting et comitologie

7.1 Reporting et comitologie CANUT

Le Titulaire doit fournir un reporting régulier de son activité et de ses résultats. Il doit identifier :

- Les bonnes pratiques qui doivent être mises en œuvre,
- Les défauts d'application des bonnes pratiques,
- Les mesures correctives à mettre en œuvre.

Un reporting devra être transmis à la CANUT tous les 3 mois, il devra notamment contenir :

- Les actions de commercialisation et leurs résultats ;
- Le volume d'affaire global réalisé et le volume d'affaire réalisé par chaque Bénéficiaire qui sera identifié par son numéro SIRET, présenté à une échelle de temps mensuelle, trimestrielle, et annuelle ;
- La liste complète des commandes passées par les Bénéficiaires ;
- La répartition des commandes annuelles sur chacune des lignes du BPU ;
- Le retour sur investissement des projets réalisés ;
- Les gains sur achats procurés aux établissements ;
- …

Ce reporting s'effectuera dans le cadre des comités de pilotage réalisés entre la CANUT et le titulaire tous les 3 mois

Le comité de pilotage se réunit en phase de lancement trimestriellement en présentiel. D'une durée prévisionnelle de 2 heures, il implique le titulaire et l'acheteur CANUT. La fréquence pour être portée semestriellement après la réalisation de 4 Comités de Pilotage.

Le titulaire sera force de proposition pour alimenter et faire évoluer cette comitologie non exhaustive.

Les indicateurs de suivi de marché seront définis lors de la réunion de lancement du marché et pourront évoluer au fil de l'eau.

D'autre part, pour chaque contrat établi entre le titulaire et le bénéficiaire, et quelques soient les unités d'œuvres souscrites, le titulaire devra fournir dans le cadre de la gouvernance de projet l'ensemble des indicateurs permettant au bénéficiaire de s'assurer du bon déroulé de la ou des missions.

Une gouvernance devra donc être mise en place au cas par cas avant le démarrage du projet.

7.2 Reporting et comitologie bénéficiaires

Le candidat décrira dans son mémoire technique et dans son Plan d'Assurance Qualité les KPI qu'il proposera au bénéficiaire. A minima, ceux-ci devront concerner :

- Des indicateurs financiers (un suivi budgétaire et une analyse détaillée des dépenses) ;
- Des indicateurs de conformité aux normes ;
- Des indicateurs liés aux projets en cours ou terminés ;

Le candidat décrira dans son mémoire technique et dans son Plan d'Assurance Qualité la comitologie qu'il entends pratiquer avec chaque bénéficiaire avec lequel il contractualise.

Article 8 Commercialisation

Le Titulaire doit assurer la promotion de l'Accord-Cadre afin que les Bénéficiaires effectifs et potentiels aient connaissance de l'Accord-Cadre et de ses caractéristiques, en faciliter l'accès et l'utilisation.

Le candidat intégrera **dans un document spécifique** les réponses aux attentes exprimés dans cet article.

Ce document doit être synthétique (50 pages maximum) et répondre précisément aux attentes ci-dessous avec des propositions concrètes. La qualité de la présentation, des réponses apportées, et le respect des consignes entreront dans la note.

Le candidat présentera :

- Les **moyens humains et matériels** qui seront mis en œuvre afin d'accroître le nombre de Bénéficiaires, et de permettre aux Bénéficiaires effectifs d'avoir des interlocuteurs qualifiés qui soient disponibles pour répondre à leurs demandes ;
- Les **campagnes de communication** permettant de développer la notoriété de l'accord-cadre qu'ils sont en capacité d'organiser durant la première année d'exécution puis les suivantes : des webinaires, des communiqués dans la presse spécialisée, la mise en avant de l'Accord-Cadre sur leur site internet, des campagnes de mailing, etc… ;
- L'organisation des **actions sur le terrain** qu'ils engageront pour faire la promotion de cet accord-cadre (organisation d'événements, démarchage direct des Bénéficiaires potentiels, etc…) ;
- La mise en avant du partenariat sur des **salons professionnels** et les outils de communication associés

Le candidat présentera sa **capacité à fournir un outillage** facilitant le processus de commande :

- Présentation de l'offre et de son contenu,
- Contacts commerciaux,
- Formulaires de contact,
- Catalogue du marché,
- Possibilité de saisir des demandes de devis en ligne, suivi des demandes, possibilité de valider une commande en ligne, etc…

Un calendrier est attendu présentant les différentes actions, leur enchaînement, leurs cibles, et les ressources du Titulaire qui les prendront en charge.

Des pénalités pourront être appliquées en cas de non-respect des engagements pris par le candidat dans sa réponse.