



APPEL A MANIFESTATION D'INTERET
CONSULTANTS
DU DISPOSITIF « DIAG CYBERSECURITE »
BPIFRANCE PARTICIPATIONS

APPEL A MANIFESTATION D'INTERET
CONSULTANTS
DU DISPOSITIF « DIAG CYBERSECURITE »
BPIFRANCE PARTICIPATIONS

1) Contexte de l'appel à manifestation d'intérêt

Bpifrance intervient auprès de ses clients sur le thème de la cybersécurité depuis quelques années via un accompagnement à la mise en place des recommandations édictées par le guide d'hygiène de l'ANSSI. Dans le cadre de ce référentiel, le niveau de maturité constaté chez les entreprises est en moyenne inférieur au niveau de maturité défini comme minimal par l'ANSSI.

Afin de remédier à ce constat, Bpifrance souhaite développer un dispositif de référence avec plusieurs objectifs :

- Diffuser de manière large auprès de ses clients les bonnes pratiques en matière de cybersécurité,
- Proposer des recommandations efficaces afin d'assurer un niveau de sécurité adéquat,
- Encourager les entreprises à investir dans leur cybersécurité.

2) Objet de l'appel à manifestation d'intérêt

Bpifrance ambitionne d'assurer entre 150 et 200 Diags Cybersécurité par an. Afin de répondre à la demande des entreprises, Bpifrance souhaite par le présent appel à manifestation d'intérêt identifier et référencer des consultants capables d'accompagner les entreprises sur tout le territoire français.

Le Diag Cybersécurité a pour objectif de proposer aux entreprises un premier niveau d'état des lieux de leur exposition aux risques ainsi qu'un plan d'actions visant à porter leur cybersécurité au niveau adéquat. Ce Diag a pour ambition de proposer un standard d'intervention pragmatique et efficace auprès des entreprises afin d'assurer un premier niveau de sécurisation.

Les consultants référencés dans le cadre du dispositif Diag Cybersécurité seront habilités par Bpifrance pendant toute la durée de fonctionnement du dispositif, sous réserve de leur engagement dans le dispositif et du respect du niveau de qualité attendu par Bpifrance.

Chaque consultant retenu dans la cadre du présent appel à manifestation d'intérêt est habilité *intuitu personae*. Il peut être salarié d'une entreprise ou être indépendant. Plusieurs consultants d'une même structure peuvent être référencés.

Les prestations ne pourront en aucun cas être sous-traitées.

3) Description du dispositif « Diag Cybersécurité »

a) Entreprises éligibles

Les entreprises éligibles au Diag Cybersécurité sont toutes les :

- Start-ups, ayant réalisé une levée de fonds de plus de 2 M€ sur les 2 dernières années (sous condition de structuration suffisante pour que le Diag soit adapté),
- Petites et Moyennes Entreprises, au sens de la réglementation européenne, c'est-à-dire dont l'effectif est inférieur à 250 personnes et le chiffre d'affaires est compris entre 2 et 50 M€
- Entreprises de Taille Intermédiaires (sous réserve de validation du périmètre de l'intervention, établie au cas par cas par Bpifrance)

Quelle que soit la taille de l'entreprise, le Diag Cybersécurité est dimensionné pour 1 seul site.

Si l'entreprise souhaite couvrir plusieurs sites, elle devra réaliser plusieurs demandes de Diag (1 Diag par numéro de SIRET).

Tout le territoire métropolitain et d'outre-mer est concerné.

Les entreprises éligibles doivent respecter la politique de Bpifrance en matière de financement des entreprises (notamment les réglementations en matière de lutte contre le blanchiment d'argent et le financement du terrorisme).

Sont exclues du dispositif : les entreprises « en difficulté » au sens de la réglementation européenne.

b) Inscription et contractualisation

Une entreprise souhaitant bénéficier d'un Diag Cybersécurité se rend sur le site Bpifrance Banque en ligne (<https://bel.bpifrance.fr/>) pour prise de renseignements et inscription en ligne au dispositif, et pourra être contactée par son chargé d'affaires Bpifrance pour obtenir des précisions.

En fonction de la demande de l'entreprise (zone géographique, activité), Bpifrance identifiera un consultant référencé sur le produit Diag Cybersécurité dans le cadre du présent AMI, validera sa disponibilité et volonté à prendre en charge la mission ainsi que l'absence de conflit d'intérêt et adressera un contrat tripartite au consultant et à l'entreprise bénéficiaire.

c) Parties prenantes

Les parties prenantes du dispositif sont les suivantes :

- Bpifrance : opérateur du dispositif Diag Cybersécurité, concepteur de la méthodologie et responsable de ses éventuelles évolutions, en charge de la constitution du vivier de Consultants habilités à réaliser le Diag Cybersécurité et garant de la qualité des prestations ;
- Le Client : bénéficiaire de la prestation ;
- Le Consultant : réalise le Diag Cybersécurité pour le compte du Client, selon les modalités définies par Bpifrance

d) Exécution de la mission

Le Diag Cybersécurité doit être exécuté suivant les deux principes essentiels exposés ci-dessous :

- **Le consultant devra appliquer la méthodologie proposée par Bpifrance, utiliser les modèles de livrables fournis et respecter les processus de gestion mis en place dans le cadre du dispositif.**
- **Le consultant s'engage à réaliser le diagnostic en toute objectivité, transparence et impartialité, sans tenir compte d'autres intérêts commerciaux.**

Les principales étapes de l'exécution de la mission sont présentées ci-dessous :

1. Préalablement à la mission

Le contrat devra être signé avant toute intervention du consultant sur le site du client. Toutes les informations relatives à l'entreprise et nécessaires à l'intervention du consultant seront précisées dans le contrat et ses annexes.

Dès réception du contrat signé par toutes les parties, le consultant appellera le client et planifiera la journée sur site. Il demandera au client la documentation disponible et utile à la préparation de la mission, telle que l'organisation du SI (si existante).

2. Journée sur site (1 jour-homme)

Les différents points ci-dessous devront être réalisés lors de la journée sur site, selon le planning le plus pertinent pour le client.

A. Journée sur site : Réunion de lancement

L'objectif de cette réunion (1/2 heure à 1 heure) est de rappeler les objectifs et contenu de la mission, de déterminer les personnes à rencontrer en entretien et de planifier la suite de l'intervention.

Le consultant complétera à cette occasion sa collecte de documents nécessaires à la suite de la prestation (si existants : organigramme, architecture du SI, politique SSI, PCA ou PRA, inventaire matériel et logiciels, procédures, etc.).

Participants :

- Consultant
- Dirigeant et responsable SI, si disponible

B. Journée sur site : Sensibilisation du Codir

Le consultant devra assurer une séance de sensibilisation du Codir, dans la mesure du possible en présentiel, afin de rappeler l'importance et les enjeux liés au risques cyber et les grands principes de protection à adopter.

Le support de cette sensibilisation sera fourni par Bpifrance au consultant et pourra être adapté à la marge, en fonction du contexte de l'entreprise. Le contenu de cette sensibilisation est adapté aux attentes d'un Codir et ne comporte pas de dimension technique poussée.

Participants :

- Consultant
- Dirigeant(s) et comité de direction, ou équivalent (et éventuellement, le responsable SI)

C. Journée sur site : Visite de site

Le consultant réalisera une visite de site (1/2h à 2h, selon les cas) afin d'observer in situ les infrastructures SI et leur niveau d'accessibilité (salle serveur, postes sensibles, équipements industriels).

Participants :

- Consultant
- Dirigeant(s) et/ou responsable SI (ou autre interlocuteur en charge de la visite)

D. Journée sur site : Entretiens

Le consultant conduira différents entretiens individuels :

- Dirigeant(s) (1h) : Compréhension de sa vision des enjeux cyber et des risques dont il a connaissance sur le marché, ainsi que de ses pratiques dans l'usage du SI. En particulier, les « Macro-actifs » IT (Informations, Services, Matériels...) critiques pour l'entreprise seront à lister avec le dirigeant, puis à confirmer / compléter lors des entretiens suivants.
- Responsable SI (1heure30) : Evaluation de la maîtrise des sujets de cybersécurité par l'entreprise et de leur bonne prise en compte dans les décisions opérationnelles, compréhension du rôle des

prestataires SI, complétion de la liste des macro-actifs IT. *Au cas où le rôle de responsable SI serait inexistant dans l'entreprise, ce créneau serait à utiliser pour un entretien avec l'un des prestataires SI et / ou d'autres employés aux fonctions proches : acheteur, maintenance, administrateur...*

- Autres entretiens – objectifs d'évaluation de leur niveau de maturité cyber, de connaissances de leurs pratiques et de complétion de la liste des macro-actifs IT (1/2h par personne) auprès de différentes populations :
 - o Utilisateurs « sensibles » (type DAF, RH ou R&D)
 - o Utilisateurs nomades (type commerciaux ou collaborateurs en télétravail)
 - o Opérateurs ou utilisateurs « type » du SI

Ces entretiens pourront être réalisés sur site, ou en visioconférence, en fonction de la disponibilité des collaborateurs.

3. Complément d'information, entretiens à distance et analyse documentaire (1,5 Jour-homme)

Le consultant passera ensuite une phase d'analyse de la documentation transmise par l'entreprise, et de recueil de compléments d'information par d'autres entretiens :

- Prestataire(s) IT pertinents
- Autres salariés
- Client(s) jugé pertinents à interviewer par le dirigeant ou le responsable SI,

Le consultant utilisera également ce temps pour compléter la grille d'évaluation de l'entreprise (format fourni par Bpifrance), ainsi que le tableau des macro-actifs IT.

Participants :

- Consultant

4. Formalisation des livrables (1 Jour homme)

Le consultant rédigera et formalisera les livrables suivant les formats de la méthodologie Diag Cybersécurité mis à disposition par Bpifrance et détaillés lors d'une formation dédiée (cf paragraphe f)) : radar et notation sur base de la grille d'évaluation, synthèse des constats forces et faiblesses par axe, recommandations et plan d'action priorisé / planifié, tableau des macro-actifs...

Participants :

- Consultant

5. Restitution du diagnostic (0,5 Jour-homme)

Le consultant restituera le contenu de son analyse au dirigeant ainsi qu'à son responsable SI (si pertinent). Les forces et faiblesses du système d'information seront présentés sur chacun des axes de l'analyse, dans un niveau de détail technique compréhensible par l'auditoire. Des recommandations d'actions seront associées à chacun de ces constats afin d'y remédier. Ces actions seront elle-même chiffrées et priorisées, en fonction de leur degré d'urgence et le niveau d'impact qu'elle pourraient avoir sur le niveau de sécurité du système d'information.

Cette restitution pourra se faire à distance ou en présentiel suivant le contexte client et les messages à passer. A la suite de cette restitution, le consultant transmettra ces livrables au client et à Bpifrance, cf. paragraphe suivant.

Participants :

- Consultant
- Dirigeant
- Responsable SI (facultatif, suivant les cas)

e) Clôture de la mission

Le consultant transmet l'ensemble des livrables de la prestation à Bpifrance et à l'entreprise bénéficiaire, c'est-à-dire :

- Le rapport de restitution de la prestation contenant : évaluation de maturité cyber de l'entreprise, détail par axe d'analyse, recommandations et plan d'actions chiffrées et priorisées, tableau des macro-actifs IT de l'entreprise et de leur sensibilité, support de sensibilisation.

Aucun compte-rendu nominatif d'entretien ne pourra être fourni par le consultant à l'entreprise.

Selon les modalités du contrat, le consultant facture l'entreprise et Bpifrance du coût de la prestation (cf contrat tripartite établi pour chaque mission).

f) Formation et outillage des consultants

Les consultants s'engagent à suivre la formation proposée par Bpifrance dans le cadre du déploiement des Diags Cybersécurité.

Cette formation vise à bâtir un socle méthodologique commun pour l'exécution des prestations et à homogénéiser les résultats obtenus. Elle permet également de mieux comprendre le contexte d'intervention, l'écosystème Bpifrance et les processus de gestion Bpifrance.

Cette formation, d'une durée d'environ une demi-journée est non-facturée et réalisée en visio. Les premières sessions auront lieu dès la première quinzaine de décembre et plusieurs sessions seront proposées afin que tous les consultants sélectionnés puissent en bénéficier.

Seuls les consultants ayant suivi la formation seront sollicités pour intervenir sur les prestations.

Suite à leur habilitation, les consultants pourront participer à des séances d'animation collective : webinaires thématiques, réunions et journées de partage d'expériences, d'ajustement de la méthodologie, etc.

g) Financement du dispositif et modalités de règlement des Diagnostics

Le consultant sera rémunéré **4 400 €HT pour 4 jours de prestation, frais de déplacement inclus.**

Le règlement de ce montant ne pourra intervenir que suite à la restitution finale et à la réception de l'ensemble des livrables de la prestation par le Client et Bpifrance.

Une partie de ce montant de 4 400 €HT sera prise en charge par Bpifrance (et/ou ses partenaires éventuels).

Le consultant adressera donc une facture à l'entreprise et une facture à Bpifrance, selon les modalités définies par Bpifrance lors de l'inscription de l'entreprise et rappelées dans le contrat de prestation signée par les trois parties.

h) Contrôle qualité et reporting

Bpifrance met en place un processus de contrôle qualité alliant des contrôles continus et des contrôles aléatoires sur la qualité des accompagnements réalisés dans les entreprises accompagnées.

Ainsi, des questionnaires de satisfaction sont administrés systématiquement aux entreprises à la suite de la restitution de la mission, afin de permettre l'amélioration continue de l'offre. Bpifrance pourra

également assister à certaines réunions clefs des prestations (réunion de lancement, visite de site, restitution).

Par ailleurs, les candidats retenus s'engagent à assurer un reporting auprès de Bpifrance sur l'avancement des missions dont ils ont la charge et leurs principaux résultats. Ce reporting sera assuré via l'envoi de questionnaires en ligne.

i) Lieu principal d'exécution du diagnostic

Les Diag Cybersécurité auront lieu pour partie au sein des entreprises souhaitant bénéficier du dispositif et pour partie en back office.

j) Délai d'exécution des diagnostics

A partir de la date de signature du contrat, l'exécution de la prestation doit être réalisée sous 3 mois maximum.

4) Caractéristiques de l'appel à manifestation d'intérêt

a) Durée et conditions de référencement des consultants

La durée de référencement des candidats retenus est égale à la durée de fonctionnement du dispositif Diag Cybersécurité, dont le démarrage de la commercialisation est prévu en décembre 2022 (pas de date de fin prévue à date).

Le consultant est habilité intuitu personae. Il peut être salarié d'une entreprise ou être indépendant. Plusieurs consultants d'une même structure peuvent être référencés.

Les prestations ne pourront en aucun cas être sous-traitées.

Bpifrance sollicitera les candidat(s) retenu(s) au cours de la durée de validité de l'appel à manifestation d'intérêt pour réaliser les Diags Cybersécurité en fonction de la demande des entreprises accompagnées.

Bpifrance ne s'engage pas à fournir un nombre minimal de Diag à chaque consultant.

Le consultant s'engage à répondre aux sollicitations de Bpifrance sous un délai d'une semaine quant à la prise en charge ou non d'une ou plusieurs prestations proposées. Il n'y a aucune obligation ou incitation à répondre positivement à chaque sollicitation, l'objectif étant de lancer rapidement les Diags Cybersécurité demandés par les entreprises bénéficiaires. Cependant en cas d'absence de positionnement du consultant sur une longue durée, Bpifrance se réserve le droit de lui retirer son habilitation.

Bpifrance se réserve également le droit de dénoncer l'habilitation à tout moment en cas de non-respect des engagements du présent cahier des charges, ou si le consultant est évalué négativement par les entreprises bénéficiaires.

Le consultant peut à tout moment renoncer à son habilitation. Un délai de prévenance de 3 mois avant fin effective de son habilitation est demandé.

Le consultant indépendant ou la structure à laquelle il appartient doit s'assurer de ne pas dépasser un taux de dépendance vis-à-vis de Bpifrance de plus de 30% de son chiffre d'affaire annuel. Au-delà de ce seuil, le consultant ou le cabinet de conseil doit en informer Bpifrance et repasser sous ce seuil dans les 6 mois suivants.

b) Critères de sélection

Les consultants candidats à cet appel à manifestation d'intérêt seront sélectionnés selon les critères suivants :

- Compréhension du contexte, objectif et enjeux du dispositif – en répondant de manière libre aux deux questions ci-dessous (cf cadre de réponse) :
 - Quels sont pour vous les principaux enjeux de la cybersécurité dans les Petites et Moyennes Entreprises ?
 - Quels arguments utiliseriez-vous pour convaincre un dirigeant de mettre en place certaines de vos recommandations suite à un Diag Cybersécurité ?
- Certifications en lien avec la cybersécurité :
 - Labels concernant le cabinet de conseil tels que PASSI de l'ANSSI (préciser les portées) ou Cyber Consultant de l'AFNOR
 - Certifications individuelles telles que CISSP, OSCP, CEH, ou autres références pertinentes,
 - Interventions dans le cadre du volet Cyber de France Relance
- Références en lien avec le Diag Cyber : si pertinent, présenter le contexte, le formalisme suivi, les recommandations proposés
 - Missions d'audit organisationnel
 - Missions d'audit technique

- Formations / Sensibilisations à destination de comité de direction
- Eventuellement, accompagnement à la mise en œuvre de mesures de remédiation
En particulier si ces interventions ont eu lieu dans des Petites et Moyennes Entreprises
- Moyens humains :
 - Niveau d'expérience du consultant
 - Autres expertises particulières pertinentes
- Couverture géographique et expertises sectorielle éventuelles

Bpifrance en tant que garant du programme d'accompagnement auprès des entreprises bénéficiaires, se réserve le droit de mener les diligences visant à vérifier la situation administrative des candidats.

c) Contenu des dossiers de candidature

Chaque dossier devra, pour être complet, comporter les éléments suivants :

- **Le CV détaillé du ou des consultant(s) mobilisé(s)** présentant leurs expériences et formations,
- S'il s'agit de salariés - une présentation rapide de la structure : année de création, équipe dirigeante, implantation(s), activité(s), effectif, etc.
- **Une présentation de votre compréhension du contexte, objectifs et enjeux**, selon les questions mentionnées dans le paragraphe précédent
- **Une présentation des références du ou des consultant(s) en lien avec le Diag Cybersécurité**, réalisées au cours des 3 dernières années précisant l'objet, la date de la mission, le destinataire, le contexte, le formalisme suivi, les recommandations proposées
- **Une présentation des certificats ou labels** relevant de la thématique du présent appel à manifestation d'intérêt,

Dans le cadre d'une entreprise présentant plusieurs candidats, il est demandé de ne joindre que **les CV des consultants fléchés pour la prestation**. Le CV de chacun des consultants (fonction, qualifications, compétences, expérience, références, zone géographique d'intervention) sera étudié individuellement.

Pour faciliter la sélection, les dossiers de candidature devront comporter les pièces suivantes :

- Un mémoire technique suivant le modèle proposé dans le présent appel à manifestation d'intérêt (document « A2_AMI-DIAG CYBER-Mémoire technique - modèle de réponse ») de 10 pages maximum et contenant en annexe les CVs des consultants et les copies des certifications et qualifications éventuelles
- Un fichier Excel de synthèse de la candidature suivant le modèle proposé dans le présent appel à manifestation d'intérêt (document « A3_AMI-DIAG CYBER-Grille de référencement »)

Nous attirons l'attention des candidats sur le fait qu'aucune proposition de collaboration alternative aux prestations communiquées dans le présent cahier des charges ne pourra être prise en compte par Bpifrance.

Pour rappel, **aucune sous-traitance ne sera possible.**

5) Calendrier de l'appel à manifestation d'intérêt

Pour la première vague de sélection :

Les candidats adresseront leurs candidatures par mail à l'adresse suivante : diagcybersecurite@bpifrance.fr **au plus tard le 25/11/2022** avec l'objet suivant « **Réponse à l'appel à manifestation d'intérêt Diag Cybersécurité** ».

La langue à utiliser dans le dossier de candidature et dans le cadre des prestations est le français.

Les dossiers qui seraient reçus par voie électronique après la date fixée ci-dessus ne seront pas retenus. Retours attendus de Bpifrance au plus tard le 09/12/2022.

Les frais de participations au présent appel à manifestation d'intérêt ne pourront pas faire l'objet d'une prise en charge par Bpifrance Participations.

Pour les candidatures déposées après la première vague de sélection et jusqu'à extinction du référencement :

Durant la période de validité du référencement, les candidats pourront adresser leurs candidatures avec les mêmes modalités que celles de la première vague de sélection, sans date butoir. Les candidatures seront analysées par Bpifrance Participation sous réserve de besoins avérés chez les entreprises bénéficiaires du dispositif.

6) Protection des données à caractère personnel

a) Protection des données à caractère personnel

Les Parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, les stipulations définies par le 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 de données à caractère personnel et à la libre circulation de ces données dit « Règlement Européen » et toute réglementation subséquente. Dans le cadre de leurs relations contractuelles, les Parties conviennent qu'elles appliqueront les dispositions reprenant les clauses contractuelles types ainsi que les annexes issues de la décision d'exécution de la commission européenne du 4 juin 2021 relatives aux relations contractuelles entre les responsables du traitement et les sous-traitants « ci-après les clauses contractuelles types ».

b) Gestion des cookies

Dans le cas où les services réalisés par le Répondant comprendraient le dépôt de cookies sur le terminal des internautes à l'initiative du Répondant, il s'engage à obtenir l'accord écrit du Client avant tout dépôt et à lui communiquer au préalable :

- la liste exhaustive des cookies envisagés ;
- la finalité précise desdits cookies ;
- la durée de validité desdits cookies, étant entendue que cette durée ne saurait dépasser treize (13) mois à compter de leur première date d'implémentation sur le terminal de l'internaute ;
 - si l'utilisation de cookies implique un traitement de données à caractère personnel. Dans cette hypothèse, les dispositions relatives aux traitements de données à caractère personnel s'appliquent, sans préjudice de l'obligation de mettre en place le système défini ci-dessous. Lorsque des cookies sont autorisés ou demandés par le Client, le Répondant s'engage à respecter la réglementation en vigueur et les recommandations de la CNIL en la matière. Le Répondant s'engage notamment à mettre en place un système de paramétrage des cookies permettant aux Utilisateurs de décider a priori d'autoriser ou non le dépôt de cookies. Les cookies publicitaires ne sont pas autorisés sur la plateforme. Le Répondant communiquera préalablement au Client les informations précitées en cas de modification(s) de l'un quelconque des cookies implémentés. Le Répondant s'engage par ailleurs à implémenter les cookies jugés nécessaire par le Client, conformément aux instructions et sous la responsabilité de ce dernier.

7) Validité des dossiers et confidentialité

Les candidats restent engagés par les éléments transmis dans leur dossier pendant une durée de 45 jours à compter de la date limite de remise de leur dossier. Aucune modification de dossier candidature n'est possible entre la date de dépôt et la date de délibération.