****

**CAHIER DES CHARGES APPEL A CANDIDATURES**

**« PRESTATAIRE MODULE TRANSFORMANT CYBERSECURITE »**

**GRAND EST**

**Date limite de dépôt des candidatures : 08/10/2025 à 23h59**

* CONTEXTE

La croissance continue de la numérisation des activités professionnelles et privées dans tous les secteurs d’activité augmente la surface d’exposition aux cyberattaques, et génère une professionnalisation et une automatisation du cybercrime, rendant le risque cyber omniprésent au sein de toutes les entités.

En conséquence, la Région a décidé d’aider les acteurs publics, associatifs et privés à mieux appréhender le risque cyber dans leur fonctionnement quotidien et comme corollaire de leur transformation numérique.

Dans ce contexte, la stratégie régionale de cybersécurité vise la résilience du territoire régional face aux cybermenaces et couvre l’ensemble du spectre du risque cyber :

* La prévention, avec l’appui aux actions de sensibilisation.
* La préparation à la crise cyber, avec le module cybersécurité (diagnostic et accompagnement à la mise en œuvre des plans d’action).
* La gestion de crise cyber et le post-traitement, avec Grand Est Cybersécurité, le centre régional d’assistance aux victimes de cyberattaques (CSIRT régional).

En parallèle, la Région Grand Est a décidé la mise en œuvre d’une dynamique d’accompagnement des entreprises personnalisée et suivie dans la durée, le parcours de transformation, qui constitue une orientation forte du SRDEII, et qui s’appuie notamment sur la mise en œuvre des transitions numérique, industrielle 5.0 et environnementale, identifiées comme des moteurs du changement et de transformation pour l’entreprise.

Les modules transformants en constituent une étape opérationnelle essentielle en ce qu’ils permettent aux bénéficiaires d’identifier la solution personnalisée qui répond spécifiquement à leur besoin ainsi que les offreurs de solutions régionaux en capacité de déployer et mettre en œuvre cette solution chez le bénéficiaire.

Le présent module s’inscrit dans cette démarche d’accompagnement.

* OBJET

L’objet de cet appel à candidature consiste à référencer les prestataires aptes à réaliser le module transformant « Cybersécurité » selon les contenus et modalités définis ci-dessous.

* Objectifs du MODULE Cybersécurité

Le module doit permettre de :

* évaluer le niveau de sécurité des systèmes d’information du bénéficiaire,
* identifier d’éventuelles failles de sécurité,
* proposer des recommandations organisationnelles (RH, process…) et/ou techniques (architecture du SI, panel de solutions techniques…) pour améliorer le niveau de cybersécurité et remédier aux failles identifiées,
* définir une feuille de route concrète et opérationnelle, adaptée au degré d’autonomie constaté (budget, ambition, compétences, …),
* accompagner l’identification de la solution technique la plus adaptée pour augmenter la cyber résilience de l’entité,
* préparer l’implémentation de la solution technique.

En termes d’organisation, plusieurs ateliers individuels et collaboratifs sont nécessaires. Considérant le caractère stratégique de la cybersécurité et l’implication de tous les collaborateurs dans sa mise en œuvre, le patronage de la direction est indispensable.

Le directeur ou des membres de l’équipe de direction doivent être impliqués dans la démarche pour garantir un succès et aboutir à des actions opérationnelles. Selon les axes d’investigation identifiés et selon la stratégie de l’entité, des personnes représentant des métiers ou des services supports sont à impliquer. Le directeur ou faisant fonction de directeur des systèmes d’information est un interlocuteur indispensable.

* Descriptif du MODULE Cybersécurité

Le module cybersécurité répond aux enjeux de la stratégie régionale en matière de cybersécurité et s’inscrit, plus particulièrement pour les entreprises du secteur industriel, BTP et logistique, dans le cadre du Parcours de Transformation de la Région Grand Est.

Le module est ouvert aux entreprises immatriculées dans le Grand Est et considérées en situation financière saine au regard de la règlementation européenne.

Le module cybersécurité se compose de 2 phases :

* La phase 1 permet, au travers du diagnostic approfondi, d’évaluer le niveau de sécurité du système d’information du bénéficiaire, d’identifier d’éventuelles failles de sécurité, tant sur le plan organisationnel que technique, et de concevoir une feuille de route définissant les travaux à mener pour renforcer les infrastructures et les systèmes et développer leur cyber résilience. Cette phase intègre la montée en compétence de l’équipe dirigeante et des principaux collaborateurs permettant une appropriation des enjeux de cybersécurité et de gestion des risques cyber.
* La phase 2 consiste en un accompagnement pour sélectionner et préparer l’implémentation des meilleures solutions de cybersécurité au regard des besoins de l’entité, en identifiant des offreurs de solutions de la communauté GET Numérique Cyber. Pour les structures concernées par la directive NIS2, cette phase s’attachera à accompagner la préparation de la mise en conformité.



* Déroulé de la méthode

La phase de montée en compétence et de diagnostic technique et organisationnel comprend

* Un questionnaire succinct transmis en amont pour pré-évaluer le niveau de maturité en cybersécurité du bénéficiaire et adapter en conséquence la conduite du diagnostic.
* Un entretien préliminaire avec le dirigeant (potentiellement d’autres membres sur invitation du dirigeant) pour bien comprendre l’organisation et les spécificités de la structure, identifier le périmètre à diagnostiquer et, si nécessaire, le cadre normatif métier. Cela permet d’élaborer le planning prévisionnel et les modalités d’exécution.
* Un audit d’organisation :
	+ Examen de la documentation interne (analyse du risque, architecture du système d’information, politique de Sécurisation du Système d’Information, Plans de Continuité/Reprise d’Activités, charte SI…)​
	+ Entretiens individuels/ateliers​.
	+ Contrôle des points clefs (référence ANSSI), analyse des résultats et recommandations.
* Livrables associés​
* Un audit technique :
	+ Tests d’intrusion/scans automatisés en boite noire avec identification des vulnérabilités et mise en exergue des vulnérabilités critiques. ​​
	+ Analyse des résultats et recommandations.
* Livrables associés​
* Finalisation :
	+ Présentation des conclusions du diagnostic. ​
	+ Élaboration d’un plan d’actions​.
* Livrables associés​

Le déroulé de cette phase ne doit pas excéder 12 semaines. Cela représente entre 4 et 8 jours/homme sur site pour une prestation de 10 jours/homme en moyenne.

Pour la phase d’ingénierie et d’identification des solutions :

En se basant sur les conclusions du diagnostic et sur le plan d’actions associé, le prestataire s’attachera à rechercher et identifier les meilleures solutions techniques existantes ou à déployer, personnalisées, au regard des besoins du bénéficiaire. Un cahier des charges de la solution préconisée sera produit assorti d’éléments financiers. Les conclusions de cette étude seront remises à l’entité bénéficiaire comme un livrable de cette phase.

Le prestataire sollicitera Grand Est Développement Solutions pour la recherche d’offreurs de solutions régionaux référencés qui seront communiqués au bénéficiaire.

Les recommandations issues de l’audit organisationnel sont reprises dans le plan d’actions remis en fin de phase de diagnostic. Sur sollicitation de l’entité bénéficiaire, le prestataire s’attachera à réaliser des entretiens avec les membres de la direction afin de les préparer au déploiement opérationnel de ces recommandations.

Le déroulé de cette phase ne doit pas excéder 16 semaines. Cela représente entre 4 et 8 jours/homme sur site pour une prestation de 10 jours/homme en moyenne.

* Missions à mener

## Le prestataire aura toute liberté pour promouvoir et communiquer autour des enjeux et contenus du module cybersécurité et prospecter les entités publiques et privées du Grand Est.

En amont du déroulé de la méthode, celui-ci devra réaliser l’ensemble des actions utiles pour que l’entité puisse réaliser le module cybersécurité en toute connaissance de cause et dans un cadre contractuel adéquat.

Les prestataires référencés devront mettre en œuvre tous les moyens à leur disposition pour mener le module cybersécurité de manière rigoureuse et exhaustive. Ils seront garants de la qualité de la prestation et de la satisfaction des clients.

Les prestataires mettront en œuvre l’ensemble des dispositions nécessaires pour assurer le suivi global du module cybersécurité par la Région Grand Est.

* Résultats attendus

Les résultats du module cybersécurité se situent à plusieurs niveaux.

**Résultats attendus** par l’entité :

* Une montée en compétence des collaborateurs aux enjeux de la cybersécurité et à la gestion des risques cyber
* L’identification des éventuelles failles de sécurité dans le système d’information
* L’identification et la priorisation des actions cyber à mettre en œuvre pour améliorer la cybersécurité
* L’identification des offreurs de solutions, prioritairement du Grand Est, qui pourront mettre en œuvre les mesures de cybersécurité préconisées, avec, sur demande de l’entreprise une mise en relation et la préparation au déploiement opérationnel de la solution.

**Livrables attendus** par le bénéficiaire du module:

* Un **rapport d’analyse synthétique** (présentation à l’attention des dirigeants et du comité de pilotage) reprenant **les principales conclusions et les recommandations critiques**. Ce rapport comportera un paragraphe consacré aux données à protéger (identification des données avec classification par degré d’importance) et à l’analyse du risque.
* Un **rapport détaillé** de la phase 1 comprenant :
	+ Les comptes-rendus des ateliers et des analyses menées pour les parties organiques et techniques;
	+ L’ensemble des recommandations et une proposition de plan d’actions.
* Un **rapport d’avant-projet détaillé** (phase 2) comprenant le cas échéant le cahier des charges de la solution et le niveau d’adaptation nécessaire, ainsi qu’une liste d’offreurs de solution en mesure de répondre à ce cahier des charges.
* Le « référentiel » intégrant un certain nombre de données prédéfinies (expressions de besoins de l’entité) qui sera transmis au prestataire lors de son référencement. Etant donné la nature confidentielle des informations touchant à la cybersécurité, il incombera au prestataire et compléter ce référentiel avec l’entité bénéficiaire et de le lui remettre. Le référentiel complété sera adressé aux services de la Région par l’entité bénéficiaire.

A noter que les rapports d’analyse attendus ont été élaborés sur la base des diagnostics de l’ANSSI (Agence nationale en charge de la cybersécurité) proposés aux collectivités dans le cadre du plan France Relance. Ils se réfèrent aux guides et documents élaborés par l’ANSSI et l’équipe en charge du portail Cybermalveillance.

* Coût de la prestation

## Le temps pour dérouler le module Cybersécurité est estimé à **20 jours / homme** s’il nécessite la mise en place des deux phases décrites précédemment (10 jours / homme en moyenne par phase).

## Le module dans son ensemble est financé à **50% du coût de la prestation** et pourra être pris en charge, dans la limite de 10 000€ HT pour la réalisation de l’ensemble des phases du module, sous réserve d’une validation par arrêté du Président, et décomposé de la façon suivante :

* Phase 1 : financement à 50%
* Phase 2 : financement à 50%
* REFERENCEMENT

## **Prestataires ciblés**

## Cet appel à candidatures s’adresse à des entreprises (TPE, PME, ETI et grands groupes, sont exclus les entrepreneurs individuels) qui pratiquent une activité de conseil dans le secteur du numérique avec des ressources humaines internalisées et une expérience significative en cybersécurité.

Les candidats doivent présenter une situation financière saine et être à jour de leurs obligations sociales et fiscales.

## **Critères de référencement**

## Il est demandé aux entreprises soumissionnaires de présenter l’adéquation de leurs ressources et de leurs expériences avec les attentes du module cybersécurité. Le référencement s’appuiera sur les critères suivants :

## Les profils des intervenants proposés, avec une attention particulière portée à l’équilibre de mixité des genres (Plan Sectoriel de Mixité Numérique de l’Etat Français, avec la Charte d’Engagement pour la mixité, l’emploi des femmes et la formation dans la filière numérique de Numeum et avec le plan pluriannuel d’actions pour l’égalité Femmes-Hommes 2023-2025 du Grand Est).

* Mentions des certifications et labels individuels et collectifs de l’entreprise (de cybersécurité et sur les technologies numériques).

## Une note d’analyse sur l’état de l’art de la cybersécurité et les défis à venir ;

## Des références justifiant d’expériences dans l’accompagnement ou la gestion de projets liés à la cybersécurité.

## Pour ce dernier point, les candidats devront justifier :

## Du nombre de projets de cybersécurité accompagnés sur les 18 derniers mois ;

## De la nature des services [préciser "Hardware", "Software", "Intégration", "Accompagnement", « Réponse aux incidents / Restauration » ou autre – plusieurs éléments peuvent être indiqués] ;

## Du secteur d’activité et de l’expertise technique [préciser un ou plusieurs aspects techniques] ;

## De la satisfaction du client qui a bénéficié de l’accompagnement ou des livrables du projet.

## Une candidature ne répondant pas à l'une de ces quelconques exigences sera écartée.

## **Procédure de référencement**

Les candidats devront adresser à la Région Grand Est le dossier de candidature dûment renseigné, complété d’éventuelles pièces complémentaires que le candidat jugerait utile d’adjoindre.

Seuls les dossiers complets seront analysés.

Sur la base des critères de référencement, l’analyse des dossiers sera réalisée par un jury composé de représentants de l’Etat, de Grand Est Développement Solutions et de la Région.

La liste définitive des prestataires retenus sera communiquée par la Région Grand Est.

Les candidats pourront être contactés durant la procédure en cas d’interrogations du jury nécessitant l’apport de précisions.

Afin de finaliser le référencement, une session d’information et de présentation du module de cybersécurité devra être suivie par l’entreprise prestataire. Seuls les prestataires justifiant de cette session pourront être définitivement référencés.

# **Durée de validité du référencement**

## Les prestataires sont référencés pour une durée de 3 ans renouvelable, sous réserve de réaliser à minima deux accompagnements cybersécurité par an.

## A l’issue de cette période de 3 ans, le prestataire doit présenter une mise à jour de son dossier sur les parties « Profils des intervenants » et « Références ».

La Région peut décider à tout moment d’écarter un prestataire qui ne répondrait à ses attentes (déontologie, contenu de l’accompagnement, niveau d’expertise, nombre d’accompagnements menés…).

* MODALITES DE CANDIDATURE

Le dossier de candidature est disponible en téléchargement sur le site Internet de la Région Grand Est : www.grandest.fr, rubrique « Mes aides régionales » ou sur simple demande à transformation@grandest.fr.

La date limite de dépôt des dossiers est le **08/10/2025 à 23h59**.

Les candidatures sont à envoyer par voie électronique à transformation@grandest.fr

* cALENDRIER

Cet appel à candidature est ouvert à compter de sa publication jusqu’au **08/10/2025 à 29h59**, date limite de dépôt des candidatures.

L’analyse des candidatures sera opérée par le jury créé par la Région. Ce jury rendra ses conclusions **avant le 08/11/2025** aux services de la Région, qui prendront contact avec les prestataires retenus pour organiser la session d’information et de présentation du dispositif.

Une fois cette session suivie les prestataires seront référencés pour être sollicités par les entreprises souhaitant bénéficier du module Cybersécurité.

* ENGAGEMENTS DU BENEFICIAIRE

Les entreprises référencées à l’issue du processus complet de référencement seront tenues à respecter les engagements suivants : vis-à-vis de la Région Grand Est et de Grand Est Développement Solutions :

* Suivre la méthodologie du module Cybersécurité telle qu’indiquée ci-dessus (partie « Déroulé de la méthode ») et présentée lors de la session d’information.
* Maintenir Faire preuve d’un agnosticisme technologique dans leurs recommandations.
* Promouvoir « prioritairement » les offreurs de solution identifiés par les GET.
* Communiquer les données, indicateurs et livrables mentionnés dans le présent appel à candidatures.
* Promouvoir le module cybersécurité auprès de leur réseau d’entreprise et de partenaires
* Garantir la satisfaction client.

Tout manquement à ces engagements fera l’objet d’une analyse approfondie par la Région Grand Est et Grand Est Développement Solutions qui pourront modifier l’avis de statut de référencement du prestataire et le notifier au prestataire concerné.

* CONFIDENTIALITE

Les entreprises soumissionnaires s’engagent par leur réponse à respecter la confidentialité des données auxquelles elles pourraient avoir accès :

* dans le cadre des échanges à l’occasion d’une éventuelle phase de négociation,
* dans le cadre de la réalisation de la prestation elle-même.

Les entreprises soumissionnaires s’engagent à ne pas utiliser ces informations pour d’autres fins que pour la réponse à la présente consultation ou pour la réalisation des prestations sollicitées, et à assurer que ces informations ne soient ni transmises, ni accessibles, à des tiers, sauf autorisation expresse et écrite par la Région.

* contact

Pour toute question relative à cet appel à projet :

|  |  |
| --- | --- |
| **Région Grand Est**Direction de la Compétitivité et de la Connaissance |  |

transformation@grandest.fr