DIAGNOSTIC CYBERSECURITE

► OBJECTIF

Pour les entreprises, la maîtrise de la gestion des risques sur leurs systèmes d'information est une condition indispensable pour réussir durablement leur transformation numérique.
Face à un accroissement des menaces cyber, la Région a engagé plusieurs actions en faveur du développement de la cybersécurité sur son territoire.

Un diagnostic Cybersécurité a été élaboré au bénéfice des entreprises régionales. Il vise à :

- améliorer la prise en compte du risque cyber et
- renforcer la prévention, la protection et la résilience des entreprises aux cyberattaques.

Il doit être pour l'entreprise qui le réalise un outil opérationnel qui permette au dirigeant :

- d'évaluer le niveau de sécurité du système d'information de son entreprise, tant sur le plan organisationnel que technique,
- d'identifier les failles éventuelles de sécurité,
- de co-concevoir une feuille de route pour améliorer la cybersécurité de l'entreprise.

► TERRITOIRE ELIGIBLE

La région Grand Est.

► BENEFICIAIRES DE L'AIDE

Les PME[1] de moins de 250 salariés, et les ETI (entreprises de taille intermédiaire)[2] immatriculées dans le Grand Est, considérées en situation financière saine au regard de la règlementation européenne[3] et à jour de leurs cotisations fiscales et sociales.

Sont exclus du bénéfice de ce dispositif : les autoentrepreneurs et microentreprises, les entreprises qui réalisent l'essentiel de leur chiffre d'affaires à partir d'une activité de négoce, les entreprises spécialisées dans les activités de conseil d'ordre juridique, financier, stratégique, ou de formation, les entreprises en procédure collective ou judiciaire.

► METHODOLOGIE DU DIAGNOSTIC

La Région Grand Est a fait construire des outils de diagnostic et une méthodologie de mise en œuvre par des experts de la cybersécurité.
Cette solution a été expérimentée sur des entreprises régionales de secteurs, tailles et besoins variés pour valider son efficacité et sa robustesse.

La Région Grand Est a référencé sur appel à candidature des prestataires qualifiés pour mettre en œuvre le diagnostic Cybersécurité selon la méthodologie retenue. Ces prestataires sont tenus à un agnosticisme technologique et ne doivent donc orienter les choix technologiques qu'en fonction des besoins de l'entreprise.

---

[1] La catégorie des PME est constituée des entreprises qui occupent moins de 250 personnes et dont le chiffre d'affaires annuel n'excède pas 50 millions d'euros ou dont le total du bilan annuel n'excède pas 43 millions d'euros (d'après l'annexe à la recommandation 2003/361/CE).
[2] Une ETI est une entreprise qui a entre 250 et 4999 salariés, et soit un chiffre d'affaires n'excédant pas 1,5 milliards d'euros soit un total de bilan n'excédant pas 2 milliards d'euros (d'après le décret ° 2008-1354 du 18 décembre 2008 relatif aux critères permettant de déterminer la catégorie d'appartenance d'une entreprise pour les besoins de l'analyse statistique et économique).
[3] A savoir notamment les entreprises faisant l'objet d'une procédure collective (ou qui en remplissent les conditions) ou qui font encore l'objet d'un plan de restructuration au sens du droit national.

Une liste des prestataires référencés est disponible sur le site de la Région Grand Est : https://www.grandest.fr/vos-aides-regionales/diagnostic-cybersecurite
Seul le recours aux prestataires référencés permet à l'entreprise de bénéficier de l'aide régionale.

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 identifié et selon la stratégie de l'entreprise, des personnes représentant des métiers ou des services supports sont à impliquer. La direction des systèmes d'information est un interlocuteur indispensable.

Déroulé de la méthode :

- Un questionnaire succinct transmis en amont pour pré-évaluer le niveau de maturité en cybersécurité de l'entreprise et adapter en conséquence la conduite du diagnostic.
- Un entretien préliminaire avec le dirigeant de l'entreprise (potentiellement d'autres membres sur invitation du dirigeant) pour bien comprendre l'organisation et les spécificités de l'entreprise, 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[4] du Système d'Information pour identifier les vulnérabilités.
    - Analyse des résultats et recommandations.
    - ⇨ Livrables associés
- Finalisation :
    - Présentation des conclusions du diagnostic.
    - Élaboration d'un plan d'actions.
    - ⇨ Livrables associés

Le déroulé de la méthode ne doit pas excéder 6 semaines. Cela représente entre 4 et 8 jours/homme sur site pour une prestation de 10 jours/homme.

[4] Le choix des outils utilisés est précisé par le prestataire

► RESULTATS ET LIVRABLES ATTENDUS

Les résultats du Diagnostic Cybersécurité se situent à plusieurs niveaux.

Résultats attendus par l'entreprise :

- Une sensibilisation des collaborateurs aux enjeux de la cybersécurité et à la gestion des risques cyber
- L'identification des éventuelles failles de sécurité dans son système d'information
- L'identification et la priorisation des actions cyber à mettre en œuvre pour améliorer la cybersécurité de l'entreprise
- L'identification des offreurs de solution notamment du Grand Est qui pourront mettre en œuvre ces actions de cybersécurité et éventuellement une mise en relation avec eux

Livrables attendus par l'entreprise :

- 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** 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.

Ces livrables 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.

Le dispositif « Diagnostic Cybersécurité » s'inscrit pour la Région Grand Est dans une nouvelle approche de l'accompagnement des entreprises, avec une relation plus suivie de chaque bénéficiaire et une collecte de données sur les prestations subventionnées afin de faire évoluer les dispositifs pour plus d'efficacité et d'efficience. Ainsi, la Région Grand Est disposera des informations suivantes de la part du prestataire ayant effectué le diagnostic Cybersécurité dans le respect des règles de confidentialité (cf. infra) :

- Nombre d'entreprises rencontrées avec présentation du diagnostic Cybersécurité
- Niveau d'intérêt pour la cybersécurité par entreprise
- Nombre de personnes ayant des compétences en cybersécurité dans l'entreprise
- Nombre et typologies des mesures de correction à prendre
- Note de maturité par entreprise
- *Nombre d'actions concrètement initiées*
- *Montant des investissements engagés pour mener la ou les mesures*
- *Nombre de mise en relation avec des offreurs de solutions en cybersécurité (discrimination des entreprises ayant leur siège en Grand Est)*
- *Nombre de personnes ayant des compétences en Cybersécurité dans l'entreprise après le Diagnostic Cybersécurité*

- Livrables attendus du diagnostic pour chaque entreprise

► METHODE DE SELECTION

Le présent dispositif fait l'objet d'une instruction par la Région.

La demande est examinée en fonction des autres demandes d'aides que le porteur a obtenues ou formulées auprès de la Région.

► DEPENSES ELIGIBLES

L'assiette éligible des dépenses est le coût hors taxe de la prestation par un prestataire référencé par la Région Grand Est. La méthodologie prévoit une **durée estimée de 10 jours / homme** pour effectuer le diagnostic Cybersécurité.

Le **coût maximum applicable** par le prestataire référencé pour réaliser le Diag Cybersécurité est de **10 000€ HT.**

► NATURE ET MONTANT DE L'AIDE

Nature : Subvention
Section : Investissement
Taux maxi : 50 % du montant de la prestation HT (dans la limite du respect du droit communautaire des aides d'état)

Plafond : 5 000 € HT

► LA DEMANDE D'AIDE

MODE DE RECEPTION DES DOSSIERS : Fil de l'eau

TOUTE DEMANDE FAIT L'OBJET D'UN DEPOT DE DOSSIER EN LIGNE SUR LE SITE WEB DE LA REGION

La demande doit comprendre le devis non signé établi par l'un des prestataires référencés par la Région Grand Est.

Des pièces complémentaires peuvent être demandées dans le cadre de l'instruction du dossier.

La date de notification d'accord de l'aide par la Région est antérieure à la date de signature du devis et de démarrage de l'opération.

Le dossier complet est instruit par les services de la Région et l'attribution de l'aide est établie par arrêté présidentiel.

► ENGAGEMENTS DU BENEFICIAIRE

Les modalités détaillées de l'instruction ainsi que les engagements du bénéficiaire figurent dans le dossier de demande d'aide à compléter selon la forme requise. A défaut, le dossier est considéré comme irrecevable. Le bénéficiaire s'engage à mentionner le soutien financier de la Région dans tout support de communication.

Le bénéficiaire s'engage à mettre en œuvre tous les moyens et ressources nécessaires pour le bon déroulé de la méthodologie du diagnostic, notamment en ce qui concerne la disponibilité des interlocuteurs au sein de l'entreprise.

Le bénéficiaire s'engage à communiquer au prestataire ou à la Région toutes les informations nécessaires au bon déroulé du diagnostic Cybersécurité et au suivi par la Région.

Ces informations resteront soumises au devoir de confidentialité des agents de la Région.

► MODALITES DE VERSEMENT DE L'AIDE

Versement unique à la fin du programme, au prorata des dépenses réalisées et par application à ces dépenses du taux d'aide fixé par le dispositif, sur présentation des livrables et données attendues par la Région et d'une copie de la facture acquittée.

► SUIVI – CONTROLE

L'utilisation de l'aide octroyée fait l'objet d'un contrôle portant sur la réalisation effective des opérations et le respect des engagements du bénéficiaire.
Le bénéficiaire s'engage à communiquer à la Région toute information relative à l'impact de l'aide régionale non couverte par le secret des affaires, afin de lui permettre de disposer des données nécessaires au suivi et à l'évaluation des politiques publiques économiques.

La Région fait mettre en recouvrement par le payeur régional tout ou partie des sommes versées de la subvention dans les hypothèses suivantes :

- manquement total ou partiel par le bénéficiaire à l'un des engagements ou à l'une des obligations issus de la convention signée,
- non présentation à la Région des documents justificatifs des dépenses engagées et acquittées.

La Région révisera le montant de la subvention à concurrence des dépenses effectivement réalisées telles que celles-ci apparaîtront au travers des justificatifs perçus.

► REFERENCES REGLEMENTAIRES

Règlement relatif à l'application des articles 107 et 108 du Traité sur le fonctionnement de l'Union européenne aux aides de minimis ou tout autre régime communautaire des aides d'état applicable en l'espèce, dont notamment pour les PME le règlement relatif au Régime cadre exempté de notification N° SA.58995 relatif aux aides à la recherche, au développement et à l'innovation (RDI) pour la période 2014-2023.

► PROPRIETE INTELLECTUELLE ET CONFIDENTIALITE DES DONNEES

La prestation vise à apporter deux types de nouvelles connaissances dans l'exécution du diagnostic de cybersécurité :

- les résultats produits par le diagnostic de cybersécurité sur la base des apports de l'Entreprise.
- les résultats issus de la mesure de la performance et de l'efficacité du diagnostic de cybersécurité.

La distribution des résultats prévoit une cession des droits d'exploitation des résultats produit par le diagnostic de cybersécurité à l'Entreprise bénéficiaire. L'Entreprise pourra librement déterminer les conditions de réutilisation des résultats, y compris pour des tiers.

La distribution des résultats prévoit une cession des droits d'exploitation des résultats issus de la mesure de la performance et de l'efficacité du diagnostic de cybersécurité à la Région. A ce titre, la Région est tenue à une exploitation confidentielle des résultats issus du diagnostic de cybersécurité en vue d'un traitement statistique anonymisé destiné, d'une part, à suivre le niveau de maturité en cybersécurité des entreprises du territoire et, d'autre part, à améliorer, en tant que de besoin, le dispositif de transformation.

► DISPOSITIONS GENERALES

- L'instruction ne débute que si le dossier est complet,

- Le versement d'une aide régionale ou son renouvellement ne constitue en aucun cas un droit acquis,

- La conformité du projet aux critères d'éligibilité n'entraîne pas l'attribution automatique de l'aide sollicitée. En effet, le Conseil Régional conserve un pouvoir d'appréciation fondé notamment sur le degré d'adéquation du projet présenté avec ses axes politiques, la disponibilité des crédits, le niveau de consommation de l'enveloppe budgétaire ou encore l'intérêt régional du projet,

- L'aide régionale ou son renouvellement ne peut être considérée comme acquise qu'à compter de la notification au bénéficiaire de la décision d'attribution prise par l'organe délibérant compétent.

Pour toute demande d'information complémentaire, nous restons à votre disposition à l'adresse suivante : diagCyber@grandest.fr