Identification

10%

Raison Sociale :

Adresse de la société :

Site(s) Web :

Vos activités :

Liste des filiales à assurer :
(Merci de préciser le pays pour chaque entité et de fournir un organigramme à jour)

Bénéficiaire(s) effectif(s)* :

Bénéficiaire effectif 1 : Nom : Prénoms : Date de naissance : Lieu de naissance : Nationalité(s) :	**Bénéficiaire effectif 2 :** Nom : Prénoms : Date de naissance : Lieu de naissance : Nationalité(s) :
Bénéficiaire effectif 3 : Nom : Prénoms : Date de naissance : Lieu de naissance : Nationalité(s) :	**Bénéficiaire effectif 4 :** Nom : Prénoms : Date de naissance : Lieu de naissance : Nationalité(s) :

**La ou les personnes physiques qui soit détiennent, directement ou indirectement, plus de 25 % du capital ou des droits de vote de la société, soit exercent, par tout autre moyen, un pouvoir de contrôle sur les organes de gestion, d'administration ou de direction de la société ou sur l'assemblée générale de ses associés.*

Avez-vous une ou plusieurs filiales basées en Polynésie française ou en Nouvelle-Calédonie ? ☐ Oui ☐ Non

Nombre d'employé total :

Chiffre d'affaires

20%

Montant du chiffre d'affaires annuel

Dernier exercice consolidé	Exercice en cours / prévisionnel	Exercice à venir
€	€	€

Répartition par zone géographique

France (y compris export EEE)	Export USA/CANADA	Export Reste du monde
€	€	€
Filiale(s) située(s) dans l'EEE	Filiale(s) située(s) aux USA/Canada	Filiale(s) située(s) dans le Reste du monde
€	€	€

Taux ou montant de marge brute d'exploitation annuel(1)

Avez-vous un/des site(s) web de commerce ou de service en ligne ? ☐ Oui ☐ Non

Si oui, merci de préciser la part de revenu généré :
[ou supporté par le ou les sites web : (% ou €)]

A titre indicatif pouvez-vous évaluer la dépendance de votre chiffre d'affaires à :

- Votre site internet représente ____ % du chiffre d'affaires annuel.
- Votre système informatique représente ____ % du chiffre d'affaires annuel.

Systèmes d'Information (SI)

30%

Nombre d'utilisateur des SI
(salariés, prestataires, partenaires… hormis les clients)

Nombre de serveurs informatiques

L'ensemble des filiales du groupe utilisent-elles le même SI ? ☐ Oui ☐ Non

Disposent-elles du même niveau de sécurité informatique que le souscripteur du contrat ? ☐ Oui ☐ Non

Si « non » à l'une des deux questions ci-dessus, veuillez remplir un questionnaire par filiale/entité, ou groupe de filiales/entités utilisant un système informatique commun ou ayant un niveau de sécurité informatique différent de celui du souscripteur du contrat.

Vos réseaux sont-ils segmentés et les sous-réseaux sont-ils capables de fonctionner indépendamment les uns des autres ? ☐ Oui ☐ Non

Si oui, merci de préciser
les solutions mise en œuvre :

Liste exhaustive des noms
de domaine possédés :

Externalisation

40%

Avez-vous externalisé certains de vos services internes auprès de prestataires tiers y compris informatiques ? ☐ Oui ☐ Non

Si oui, avez-vous mis en place des procédures pour vérifier les contrôles de sécurité et de confidentialité de vos fournisseurs informatiques lors de la passation de vos marchés ? ☐ Oui ☐ Non

Si oui, faites-vous annuellement des audits de cybersécurité chez ces prestataires ? ☐ Oui ☐ Non

Tous vos recours sont-ils maintenus auprès de ces sous-traitants et prestataires ainsi que leurs assureurs ? ☐ Oui ☐ Non

Vérifiez-vous que ces sous-traitants et prestataires sont assurés contre les cyber-risques ? ☐ Oui ☐ Non

Externalisez-vous partiellement ou totalement l'hébergement de vos Systèmes Informatiques ? ☐ Oui ☐ Non

Si oui, confirmez-vous que votre hébergeur s'engage à vous fournir une disponibilité au moins égale à 99.9% et est certifié ISO27001 et héberge vos Systèmes Informatique dans deux ou plusieurs datacenter situés à plus de 350km les uns des autres ? ☐ Oui ☐ Non

Protection des Données Personnelles (DP)

50%

Nombre de données sensibles* collectées ou détenues :
*Données sensibles : 1. Numéro de sécurité sociale, permis de conduire ou passeport. 2. Données bancaire (carte de crédit, etc.)
3. Données relatives à la race, l'ethnie, l'orientation sexuelle, la santé, les convictions religieuses ou philosophiques, les opinions politiques, les engagements syndicaux.

≤ 20.000	☐	1.000.001 - 2.000.000	☐
20.000 - 100.000	☐	2.000.001 - 3.000.000	☐
100.001 - 250.000	☐	3.000.001 - 4.000.000	☐
250.001 - 500.000	☐	4.000.001 – 5.000.000	☐
500.001 - 1.000.000	☐	> 5.000.000	☐

Collectez-vous des données de santé ? ☐ Oui ☐ Non

Si oui, l'hébergeur de ces données est-il certifié HDS (5) ? ☐ Oui ☐ Non

Disposez-vous d'une politique de traitement et de protection des DP formalisée, conforme aux lois et réglementations en vigueur, validée par la Direction et diffusée à l'ensemble de vos salariés ? ☐ Oui ☐ Non

Avez-vous désigné un Correspondant Informatique et Libertés ou un Data Protection Officer (DPO), en interne ou externe ? ☐ Oui ☐ Non

Vos salariés ayant accès à des données sensibles sont formés aux règles de sécurité concernant l'accès, le traitement et la transmission des données au moins 1 fois par an ? ☐ Oui ☐ Non

Les données que vous stockez sont-elles cryptées ? ☐ Oui ☐ Non

Si oui, avec quel type de cryptage (recommandé 256bits) ?

Les données en transit sur votre réseau sont-elles cryptées y compris en cas d'accès distants par VPN ? ☐ Oui ☐ Non

Si oui, avec quel type de cryptage (recommandé 256bits) ? ☐ Oui ☐ Non

Acceptez-vous les paiements par carte bancaire ?

Si oui, merci de compléter les questions ci-dessous :
Nombre de transactions par carte bancaire et par an

≤ 20.000	☐	1.000.001 - 2.000.000	☐
20.000 - 100.000	☐	2.000.001 - 3.000.000	☐
100.001 - 250.000	☐	3.000.001 - 4.000.000	☐
250.001 - 500.000	☐	4.000.001 – 5.000.000	☐
500.001 - 1.000.000	☐	> 5.000.000	☐

Êtes-vous le responsable du traitement de ces données ? ☐ Oui ☐ Non

Si oui, êtes-vous conforme au dernier standard PCI-DSS ? ☐ Oui ☐ Non

Si non, veuillez indiquer le nom de votre fournisseur et préciser les mesures de sécurité mise en place

Management des accès à vos Systèmes d'information

60%

Chaque utilisateur dispose d'un identifiant et mot de passe unique ? ☐ Oui ☐ Non

Fournissez-vous un accès à distance aux systèmes informatiques pour vos utilisateurs ? ☐ Oui ☐ Non

Quelle politique de limitation des privilèges et des accès aux systèmes informatiques appliquez-vous ? (plusieurs cases possibles)

- ☐ Pas de limitation des droits d'accès
- ☐ Seul les utilisateurs en ayant besoin dispose de privilèges administrateurs (6)
- ☐ Principe du moindre privilège (7)

Les administrateurs (6) possèdent-ils tous deux comptes : un pour leurs missions d'administrateurs et un autre pour les usages quotidiens ? ☐ Oui ☐ Non

Avez-vous recours à la vérification en deux étapes - A2F/MFA – (8) pour gérer les accès à distance et/ou les accès à des application web :

- ☐ Pour tous vos utilisateurs ?
- ☐ Pour les administrateurs (6) ?
- ☐ Pour vos fournisseurs et prestataires extérieurs ?

A défaut, envisagez-vous de déployer ce type de contrôle et pour quelle catégorie d'utilisateur ? ☐ Oui ☐ Non

Si oui, quand ?

Les accès des préposés sont-ils systématiquement coupés lorsqu'ils quittent votre entreprise ? (dans les 3 mois au plus tard suivant leur départ) ☐ Oui ☐ Non

Faites-vous des audits au-moins annuels pour contrôler l'efficacité de votre politique d'attribution des privilèges d'accès ? ☐ Oui ☐ Non

Disposez-vous d'accès à distance aux systèmes de vos clients ? ☐ Oui ☐ Non

Si oui, fournissez-vous l'un des services suivants à vos clients ?

- ☐ Gestion des sauvegardes
- ☐ Administration et gestion des solutions de gestion des identités et des accès, telles que Active Directory
- ☐ Gestion de la cybersécurité
- ☐ Gestion du courrier électronique

Sécurité des systèmes informatiques

70%

A- Politique de sécurité et gestion des risques

Qui est responsable de la sécurisation des données et de systèmes informatiques ?

- ☐ **Responsable IT**

☐ Directeur Général ou équivalent
☐ RSSI
☐ Autre

Menez-vous des formations au moins une fois par an à la cybersécurité pour tous vos salariés ? ☐ Oui ☐ Non

Réalisez-vous des campagnes de phishing auprès de vos salariés ? ☐ Oui ☐ Non

Faites-vous des audits annuels de la sécurité de vos systèmes informatiques ? ☐ Oui ☐ Non

Si oui, sous quel délai maximum mettez-vous en œuvre les recommandations :

B- Protection des Systèmes Informatiques

Un antivirus est-il installé sur tous les systèmes informatiques ? ☐ Oui ☐ Non

Déployez-vous les patchs de sécurité pour vos logiciels et systèmes (y compris antivirus et pare-feu) suivant la mise à disposition par le fabricant :

☐ Oui dans un délai inférieur à 30 jours,
☐ Oui dans un délai supérieur à 30 jours
☐ Oui automatiquement
☐ Non

Les correctifs et nouveaux codes sont-ils testés dans un environnement de test distinct avant déploiement dans l'environnement réel ? ☐ Oui ☐ Non

Disposez-vous de systèmes d'exploitation dont les mises à jour ne sont plus supportées par leur fabricant ? ☐ Oui ☐ Non
(par exemple Windows XP, Windows 7, Windows serveurs 2008, etc…)

Si oui:
Si une extension de support est disponible, a-t-elle été achetée pour ces systèmes ? ☐ Oui ☐ Non

Les systèmes concernés sont-ils connectés à internet ? ☐ Oui ☐ Non

Sont-ils totalement segmentés des autres systèmes ? ☐ Oui ☐ Non

Si non :
Quels sont les moyens de protection mis en œuvre ?

Sous quel délai une migration est-elle prévue ?

C- Sauvegardes

Réalisez-vous des sauvegardes de l'ensemble de vos systèmes et données ? ☐ Oui ☐ Non

A quelle fréquence sont-elles réalisées ?

☐ Quotidienne

☐ Hebdomadaire

☐ Mensuelle

☐ Autre : _____

Vos sauvegardes sont-elles déconnectés de votre réseau ? ☐ Oui ☐ Non

Utilisez-vous un système de synchronisation cloud pour vos sauvegardes ? ☐ Oui ☐ Non

Vos sauvegardes sont-elles immuables ? ☐ Oui ☐ Non

L'accès à vos sauvegardes est-il possible uniquement aux comptes administrateurs ? ☐ Oui ☐ Non

Les sauvegardes sont-elles accessibles uniquement par l'utilisation d'une authentification unique ou d'une solution à facteurs multiples A2F/MFA(8) ? ☐ Oui ☐ Non

Vos procédures de sauvegardes suivent-elles la «règle 3/2/1» (10) ? ☐ Oui ☐ Non

Vos sauvegardes sont-elles testées ? ☐ Oui ☐ Non

Si oui, a quelle fréquence:

☐ Mensuelle

☐ Trimestrielle

☐ Annuelle

☐ Les tests sont espacés de plus d'un an

Pour quelle période conservez-vous vos sauvegardes :

☐ Moins de 30 jours

☐ Entre 30 et 90 jours

☐ Plus de 90 jours

D- Sécurité et surveillance des réseaux

Des pares-feux sont-ils déployés pour réguler le trafic réseau ? (plusieurs cases possibles)

☐ Périmètre du réseau

☐ Tous les postes utilisateurs et les extrémités du réseau

☐ Aucun pare-feu n'est déployé

Avez-vous déployé un Web Application Firewall (WAF) pour protéger l'ensemble des applications en contact avec l'extérieur ? ☐ Oui ☐ Non

Des outils de sécurité des points d'accès (EDR - Endpoint Detection & Response) sont-ils déployés sur :

☐ Les postes de travail ?

☐ Les serveurs ?

Avez-vous mis en place des mesures pour détecter toute attaque, tentative d'attaque ou incident de sécurité ? ☐ Oui ☐ Non

Conservez-vous les fichiers journaux (Log) pour une durée minimale de 90 jours ? ☐ Oui ☐ Non

Réalisez-vous une sauvegarde de vos Logs ? ☐ Oui ☐ Non

Disposez-vous de l'une des solutions suivantes :

☐ SOC (Security Operations Center) géré par une équipe interne à l'entreprise

☐ SOC externe

☐ SIEM (Security Information and Event Management)

☐ Autres :

Si vous disposez d'un SOC, est-il disponible 24h/24 et 7j/7 ? ☐ Oui ☐ Non

Conduisez-vous des tests de pénétration au moins une fois par an ? ☐ Oui ☐ Non

Conduisez-vous des tests d'analyse de vulnérabilité au moins une fois par an ? ☐ Oui ☐ Non

Sous-quels délais procédez-vous à la mise en œuvre du plan de remédiation s'avérant nécessaires suite à ces tests ?

E- Résilience des systèmes informatiques

Bénéficiez-vous d'une ou plusieurs certifications en rapport avec la sécurité informatique ou les bonnes pratiques en la matière ?

☐ ISO27001, ou équivalent, préciser :

☐ HDS

☐ Autres, préciser :

Disposez-vous d'un Plan de Reprise d'Activité (PRA) et d'un Plan de Continuité d'Activité (PCA) en cas d'incident sur vos Systèmes Informatique tel qu'une attaque par Ransomware ? ☐ Oui ☐ Non

Votre PRA et PCA sont-ils testés ? ☐ Oui ☐ Non

Hébergez-vous partiellement ou totalement vos Systèmes Informatiques ? ☐ Oui ☐ Non

Avez-vous mis en place une architecture redondante ? ☐ Oui ☐ Non

Votre réseau est-il segmenté et chaque segment capable d'opérer indépendamment des autres ? ☐ Oui ☐ Non

Commentaires

80%

Avez-vous des précision ou tout commentaire à porter ou document à joindre pour nous aider à mieux appréhender votre stratégie et dispositif de sécurité informatique ?

Utilisation de systèmes opérationnels

90%

Utilisez-vous dans le cade de vos activités des systèmes de type ICS/SCADA/DCS ? ☐ Oui ☐ Non

Cyber-Fraude :

(Fraude réalisée exclusivement via une intrusion dans le Système informatique)

100% : N'oubliez pas de sauvegarder !

Existe-t-il une procédure de double signature/validation pour les paiements supérieurs à 10.000 € ? ☐ Oui ☐ Non

A défaut :

☐ Une procédure de double signature/validation est requise pour des paiements supérieurs à : …… €

☐ Aucune procédure de double signature/validation n'est jamais requise.

Les fonctions d'ordonnancement et de paiement sont séparées au sein de votre organisation ? ☐ Oui ☐ Non

Utilisez-vous des applications sécurisées avec MFA (8) dans le cadre de vos ordres de paiement, avec envoi des codes temporaires de validation autrement que par email ? ☐ Oui ☐ Non

Antécédents :

Durant les 3 dernières années, avez-vous subi un sinistre d'un coût total supérieur à 1.500 € (que celui-ci ait été indemnisé ou non) ? ☐ Oui ☐ Non

Si oui, préciser le montant, la date, les faits (vulnérabilité exploitée, vecteur, conséquences)et mesures mises en place pour s'en prémunir à l'avenir, ainsi que le calendrier de déploiement de ces mesures :

Avez-vous fait l'objet d'une enquête de la CNIL (ou son équivalent à l'étranger) ? ☐ Oui ☐ Non

Si oui, fournir les détails :

Avez-vous connaissance d'événements ou circonstances pouvant donner lieu à la mise en jeu de la garantie ? ☐ Oui ☐ Non

Si oui, fournir les détails (dates et faits) :

Avez-vous déjà été assuré en cyber auprès d'Hiscox ou avez-vous demandé une proposition d'assurance au cours des 3 derniers mois? ☐ Oui ☐ Non

Glossaire non contractuel :

(1) **Marge brute d'exploitation :** schématiquement et suivant le plan comptable, il s'agit de la différence entre les produits d'exploitations HT d'une part (comptes 70, 71 et 72) et les charges variables d'exploitation HT d'autre part (comptes 601, 6021, 6026, 607, 6241 et 6242) ; charges variables dont il faut retrancher les rabais, remises et ristournes (compte 609), ainsi que la variation des stocks (comptes 6031, 6032 et 6037).

(2) **Données sensibles :** au sens du Règlement européen sur la protection des données personnelles

(3) **DMZ :** en cybersécurité, une DMZ (zone démilitarisée) est un sous-réseau qui héberge les unités et/ou serveurs d'une entreprise accessibles ou visibles depuis internet, donc plus exposés. La DMZ agit en zone tampon séparée du réseau interne par un second firewall, séparant donc techniquement le réseau interne du réseau exposé à internet.

(4) **Les données et systèmes critiques** sont définis comme ceux dont l'indisponibilité ou le maintien hors ligne plus de 24 heures, engendreraient pour vous une perte de revenus

(5) **Niveau de Tier et Certification HDS :** le niveau de Tier est indiqué par votre prestataire d'hébergement, il se classe en niveaux de 1 à 4, 4 étant le plus élevé. La certification HDS (Hébergement données de santé à caractère personnel) est nécessaire dès que vous recueillez à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social des données de santés.

(6) **Administrateur :** une session **administrateur** permet notamment de modifier des paramètres de sécurité, installer/désinstaller des logiciels et des composants matériels, accéder à tous les fichiers de l'ordinateur et/ou du réseau et procéder à des modifications sur les autres comptes d'utilisateurs.

(7) **Politique de moindre privilège :** les utilisateurs de votre système informatique n'ont accès qu'aux applications et données strictement nécessaires à l'exécution de leur mission, en d'autres termes ne sont accordés que les minimums requis à l'exercice de leur mission.

(8) **Authentification à double facteurs/à multiple facteurs (A2F/MFA)** : au-delà du nom d'utilisateur et du mot de passe, s'ajoute la réception d'un code de sécurité que seul l'utilisateur authentique pourra recevoir sur son téléphone, sa messagerie ou une application spécifique d'authentification.

(9) **WAF (Web application Firewall) :** un WAF est un dispositif de sécurité essentiel protégeant les applications Web qui ont leurs vulnérabilités spécifiques. Il se distingue du pare-feu classique qui est lui placé au niveau du périmètre de votre réseau.

(10) **Règle de sauvegarde 3/2/1 :** elle signifie que vous devez disposer de **3** copies de vos données, sur **2** supports différents, et conserver au moins 1 copie de sauvegarde hors site. C'est une pratique gage de résilience notamment face aux attaques de type ransomware par cryptage des données.

Assurance

Date de prise d'effet souhaitée : ☐ Echéance souhaitée : ☐

Déclaration **Utilisation de vos données personnelles**

HISCOX est le nom commercial de plusieurs sociétés du groupe HISCOX. La société intervenant en qualité de responsable du traitement de vos données à caractère personnel figure sur la documentation qui vous est fournie. Pour toute question, vous pouvez nous contacter en nous envoyant un courriel à dataprotectionofficer@hiscox.com, ou en nous écrivant à Immeuble Le Millenium, 12 quai des Queyries, CS 41177, 33072 BORDEAUX CEDEX

Nous collectons et traitons des informations vous concernant aux fins de proposer et d'exécuter des contrats d'assurance, et de pouvoir traiter vos réclamations. Vos données sont également utilisées à des fins opérationnelles, telles que la prévention et la détection des fraudes, ainsi que la gestion financière.

Nous pouvons ainsi être amené à collecter ou à partager vos données avec des sociétés de notre groupe et à des tiers, tels que les courtiers, les experts, les agences de renseignement économique, les prestataires, les conseillers professionnels, nos régulateurs ou les agences de lutte contre la fraude.

Nous ne conservons pas vos données au-delà du temps nécessaire à l'accomplissement de l'objectif poursuivi par leur collecte et dans le respect des dispositions législatives et réglementaires applicables.

Vos appels téléphoniques sont également susceptibles d'être enregistrés, afin de nous aider à surveiller et à améliorer nos services.

Vous bénéficiez d'un droit d'accès, de rectification ou d'effacement de vos données personnelles, et d'un droit d'opposition à leur traitement. Pour de plus amples informations, nous vous invitons à consulter notre politique de confidentialité https://www.hiscox.fr/cookies-et-confidentialite .

Déclaration

Je soussigné(e) _____

déclare qu'à ma connaissance, **tous les renseignements donnés**, que le questionnaire ait été rempli **de ma main ou de celle de mon mandataire, sont exacts**.

Je reconnais être informé(e) de **l'obligation de sincérité des réponses** au présent questionnaire et des conséquences **qui résulteraient d'une omission ou d'une fausse déclaration**, à savoir la nullité du contrat (Article L 113-8 du Code des Assurances) ou **la réduction des indemnités** (Article L 113-9 du Code des Assurances). En signant cette déclaration, je ne suis pas tenu(e) d'accepter les termes de la proposition d'assurance faite par les assureurs, mais **dans le cas où un contrat serait accepté, les déclarations faites dans ce questionnaire feront partie intégrante du contrat et lui serviront de base.**

Fait à _____

Le _____ / / _____

Signature _____