[Annexe 11. Dispositif de Maîtrise des Risques (« DMR »)]

Au regard de l'exposition aux risques des Prestations pour l'Acheteur, le Titulaire s'engage à mettre en place un dispositif de surveillance et de maîtrise des risques des Prestations et à rendre compte régulièrement à l'Acheteur du détail des éléments de ce dispositif, y compris leur efficacité.

En conséquence, le Titulaire s'engage, en particulier, à fournir à l'Acheteur les éléments suivants de surveillance et de maîtrise des risques, relatifs aux Prestations, conformément aux articles « Dispositions relatives à l'externalisation des Prestations », « Audit » et « Sous-traitance » des pièces contractuelles du Marché.

Eléments à fournir à l'Acheteur au moins une fois par an :

- Documents faitiers relatifs à la gouvernance et à la mise en œuvre de la SSI : PSSI, gestion des accès et des habilitations, gestion et application des correctifs de sécurité, …

- Toutes attestations et certifications SSI pertinentes au titre de l'exécution de la Prestation (PCI-DSS, ISO27001, Hébergeur de Données de Santé, SecNumCloud, ISAE3402 Type 1 et Type 2, *etc.*) ;

- L'attestation ISAE2402 :
    - En l'absence de certification ISAE3402 Type 1 et Type 2, fournir les éléments démontrant la mise en œuvre par le Titulaire et l'efficacité d'un dispositif de contrôle interne avec notamment l'établissement de la cartographie des risques, de plans de contrôle (niveau 1 et niveau 2) et de plans d'action afférents.
      Nota bene : A ce sujet, il est demandé au Titulaire de démontrer la mise en œuvre effective et l'efficacité d'un contrôle interne, il n'est pas demandé de produire le dispositif de contrôle interne lui-même.

- Le descriptif du Plan d'Urgence et de Poursuite d'Activité et la synthèse des tests annuels de mise en œuvre du Plan d'Urgence et de Poursuite d'Activité du Titulaire (comprenant le Plan de Secours des Systèmes d'Information et le Plan de Secours des Activités), ou autres tests relatifs à démontrer la résilience opérationnelle, ainsi que les mesures correctives mises en œuvre au regard des Anomalies détectées. Par ailleurs, le Titulaire communique tous les documents et informations prévus à l'annexe « Plan d'Urgence et de Poursuite de l'Activité ».

- Le suivi des mesures de remédiation mises en œuvre sur les Incidents liés aux TIC survenus au cours de l'année concernée et qui ont impacté l'Acheteur.

- S'agissant des Sous-Traitants du Prestataire :

Interne

- L'actualisation, le cas échéant, de l'Annexe Sous-traitance et lieux d'exécution de la Prestation par le Titulaire et ses Sous-Traitants ;
- Les indicateurs de niveau de services convenus entre le Prestataire et ses propres sous-traitants ;
- L'actualisation des pièces d'évaluation des risques liés à la sous-traitance ultérieure du Prestataire.

En cas de concession de droit d'utilisation (licence) portant sur un logiciel :

- Production du certificat d'entiercement auprès d'un séquestre des codes sources mentionnant le Client désigné comme bénéficiaire du séquestre.

- Produire annuellement les attestations d'audit de sécurité (comprenant notamment les audits de code et les pentest).

Eléments à fournir à l'Acheteur au moins quatre fois par an :

- Rapport sur les indicateurs de qualité de services, lors des comités de suivi de la Prestation ou *a minima* trimestriellement, y compris les indicateurs relatifs au suivi des corrections des vulnérabilités.

La liste ci-dessus pourra être complétée par l'Acheteur au cours de l'exécution du Marché pour lui permettre notamment (i) de respecter ses obligations légales et règlementaires liées à la réévaluation du profil de risque existant et (ii) de mettre en œuvre les dispositions de l'article « Audit » du Marché, en particulier pour vérifier le respect des normes de performance et de qualité appropriées et traduire des recommandations issus des audits diligentés conformément audit Article « Audit » du Marché.

Interne