Annexe 4. 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.*) ;

- 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.

- les rapports de tests de pénétration du SI que le titulaire a pu réaliser, ainsi que ceux de ses sous-traitants ;

- le prestataire devra fournir (**sur demande et une fois par an**) toutes réponses relatives aux critères d'appréciation des objectifs de sécurité qui le concerne. La Caisse des Dépôts peut exercer un droit de contrôle (sur pièce et sur place) sur le prestataire à sa propre initiative et quand elle le juge utile dans le cadre des contrôles de premier et second niveau relatifs au périmètre de l'activité sous-traitée.

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.

Interne

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