

Cahier des Clauses Techniques Particulières (C.C.T.P.)

Prestations d'accompagnement à la conformité réglementaire et conseil juridique

DATE LIMITE DE RÉCEPTION DES OFFRES :

17/07/2026 à 12h00

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

Attention : Les zones entourées de crochets [] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

Erreur ! Source du renvoi introuvable.

Table des matières

Présentation du Projet.....	4
1.1 Le client.....	4
1.2 Contexte et Besoins	4
2 Détail de l'appel d'offre	5
2.1 Périmètre de l'appel d'offre	5
2.2 Durée du Marché.....	5
2.3 Déroulement de la consultation	5
2.4 Services adaptés au GRADeS BFC	5
2.1 Sécurisation des échanges	6
2.2 Réalisation des Prestations.....	6
2.3 Validation des prestations	6
2.4 Bordereau de prix	6
2.5 Processus de commande de prestations et paiement des factures	6
2.6 Renseignements.....	7
3 Lot 1 : Accompagnement au système de management intégré (SMI).....	7
3.1 Besoin.....	7
3.1.1 Périmètre des prestations.....	7
3.1.2 Cas d'usage pour l'analyse des offres.....	8
3.2 Suivi et Evaluation.....	10
3.3 Capacités individuelles exigées.....	10
3.4 Références Clients	11
3.5 Références groupes de travail spécialisés.....	11
4 Lot 2 : Audit Interne	12
4.1 Besoin.....	12
4.2 Exigences Normatives.....	12
4.3 Exigences compétences / expertises.....	13
4.4 Définitions à utiliser	13
4.4.1 Point fort (PF) :	13
4.4.2 Piste de Progrès (PP) :	13
4.4.3 Point Sensible (PS) ou Point de Vigilance (PV) :	13
4.4.4 Non-conformité Mineure (NC. Min.)	13
4.4.5 Non-conformité Majeure (NC. Maj.)	14
4.4.6 Note :	14

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

Attention : Les zones entourées de crochets [] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

Erreur ! Source du renvoi introuvable.

4.5	Plan d'audit.....	14
4.6	Fiches de non-conformité.....	15
4.7	Propositions d'actions.....	15
4.8	Références Clients.....	15
5	Lot 3 : Accompagnement juridique et réglementaire en lien avec l'intelligence artificielle, les technologies innovantes et le SMI et Règlementaire.....	16
5.1	Besoin.....	16
5.2	Accompagnement juridique et réglementaire.....	16
5.3	Veille légale et réglementaire.....	17
5.4	Compétences / Expériences.....	18
5.5	Suivi et Evaluation.....	19
6	Lot 4 : Accompagnement juridique et réglementaire spécifiques aux règles de la fonction publique	19
6.1	Besoin.....	19
6.2	Assistance juridique.....	20
6.3	Compétences / Expériences.....	20

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

Attention : Les zones entourées de crochets [] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

Erreur ! Source du renvoi introuvable.

Présentation du Projet

1.1 Le client

Le GIP GRADeS BFC a été créé le 5 septembre 2019 sous le statut de GIP de droit public.

En reprise des activités historiques des GCS EMOSIST et e-Santé Bourgogne depuis le 1er janvier 2020, il a en charge la gestion, le développement et le déploiement des systèmes d'information de santé pour la région de Bourgogne Franche-Comté.

Il est actuellement composé de plus de quatre-vingt agents répartis sur les domaines administratifs, techniques et fonctionnels, rattachés sur 3 sites.

Dans le cadre de ses activités le GRADeS BFC est certifié ISO 9001 :2015, ISO 27001 :2022 et Hébergeur de données de santé V2.

La certification Hébergeur de données couvre les 6 activités du référentiel.

1.2 Contexte et Besoins

L'organisation est engagée dans une démarche structurée de management de la qualité et de la sécurité de l'information, s'appuyant notamment sur un Système de Management Intégré (SMI) couvrant les dimensions qualité, sécurité de l'information et conformité réglementaire.

Ce SMI s'inscrit dans une logique d'amélioration continue et vise à garantir la maîtrise des processus, la conformité aux exigences normatives et réglementaires applicables, ainsi que la satisfaction des parties prenantes.

Dans ce cadre, l'organisation souhaite renforcer et faire évoluer son SMI afin d'en améliorer l'efficacité, la cohérence documentaire, l'appropriation par les équipes et l'adéquation avec les exigences réglementaires et normatives en vigueur. Cette démarche d'amélioration continue concerne notamment la structuration et l'optimisation des processus, l'évolution du corpus documentaire qualité, ainsi que l'alignement du dispositif avec les bonnes pratiques reconnues.

Par ailleurs, certaines thématiques nécessitent un accompagnement spécialisé en matière juridique, notamment pour sécuriser l'interprétation et l'application des obligations réglementaires, contractuelles et normatives applicables aux activités de l'organisation. Cet appui vise à garantir la conformité des dispositifs, des documents contractuels et des pratiques internes avec le cadre juridique en vigueur.

Le présent marché a pour objet de recourir à des prestations intellectuelles, d'appui et de conseils juridiques adaptées aux enjeux et évolutions du GRADeS. Ces prestations s'articulent autour des axes suivants :

- Le pilotage et l'animation du système de management de la qualité (SMI) (Lot1)
- La réalisation d'audit interne de conformité (Lot2)
- L'accompagnement juridique opérationnel (Lot3)
- L'accompagnement juridique et réglementaire spécifique aux règles de la fonction publique (Lot 4)

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

Attention : Les zones entourées de crochets [] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

Erreur ! Source du renvoi introuvable.

2 Détail de l'appel d'offre

2.1 Périmètre de l'appel d'offre

Cet appel d'offre est un marché à bons de commande constitué de 4 lots, définis comme suit :

- Lot 1 : Accompagnement au système de management intégré (SMI)
- Lot 2 : Audit Interne du SMI
- Lot 3 : Accompagnement juridique et réglementaire en lien avec l'intelligence artificielle, les technologies innovantes et le SMI
- Lot 4 : Accompagnement juridique et réglementaire spécifiques aux règles de la fonction publique

Un même opérateur économique peut soumissionner pour un ou tous les lots.

Un bordereau de prix unitaire est attendu de la part du prestataire pour chacun des lots.

Le candidat pourra proposer en option à la réponse toutes prestations et outillages complémentaires qu'il jugera utile.

2.2 Durée du Marché

La durée du marché est de 1 an reconductible 3 fois.

En cas de non-reconduction le GRADeS notifiera le candidat 2 mois avant la date anniversaire du contrat.

2.3 Déroulement de la consultation

Le marché est constitué de 4 lots. Le candidat peut répondre à un ou plusieurs lots. Il peut recourir à la sous-traitance, mais reste maître d'œuvre et responsable du projet.

La sélection des candidats sera réalisée en deux étapes.

- Etape 1 : Analyse des offres sur la base des documents fournis par les candidats
- Etape 2 : Notation finale

2.4 Services adaptés au GRADeS BFC

Le candidat devra démontrer que sa démarche permet d'assurer une réponse couvrant les besoins du GRADeS BFC.

Le candidat décrira sa compréhension des besoins et des enjeux de ce marché et des contraintes identifiées le cas échéant.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

Attention : Les zones entourées de crochets [] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

Erreur ! Source du renvoi introuvable.

Il lui appartient de décrire/présenter/apporter les preuves de sa méthodologie pour l'exécution du marché, ainsi que les outils associés, notamment des exemples anonymes de :

- Calendrier prévisionnel du projet ;
- Méthodologie d'analyse de risque ;
- Grille d'analyse ;
- Rapport d'audit ;
- Guide d'entretien ;
- Tableau des non-conformités ;
- Tout autre document utilisé lors de la prestation pour l'exécution du marché.

Le candidat indiquera les documents qui lui seront nécessaires pour démarrer l'exécution du marché.

2.1 Sécurisation des échanges

Le prestataire détaillera dans son offre les modalités proposées pour sécuriser les échanges de données afin de garantir notamment la confidentialité et l'intégrité des données.

2.2 Réalisation des Prestations

Les prestations pourront se dérouler à distance ou sur les sites du GRADeS BFC.

Le candidat devra préciser dans son offre les modalités de déplacement et les coûts associés.

Chaque prestation devra donner lieu à un livrable qui devra répondre aux exigences demandées.

2.3 Validation des prestations

Pour chaque prestation, le prestataire justifiera du temps passé sur chaque mission et fournira un relevé d'activité qui servira de justificatif pour le paiement des factures associées.

2.4 Bordereau de prix

Le candidat devra fournir un bordereau de prix unitaire qui devra préciser le coût horaire et le coût journalier des profils proposés.

Il précisera également les modalités de facturation en cas de déplacements sur site.

2.5 Processus de commande de prestations et paiement des factures

Chaque sollicitation du GRADeS BFC sera matérialisée par une demande écrite envoyée par mail définissant le périmètre de la prestation, et les livrables attendus.

Le prestataire devra fournir en retour un devis estimant la charge nécessaire pour la réalisation de la prestation.

A partir de ce devis un bon de commande GRADeS BFC sera envoyé au prestataire ce qui déclenchera le lancement de la prestation.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

Attention : Les zones entourées de crochets [] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

Erreur ! Source du renvoi introuvable.

La prestation devra être validée par le GRADeS BFC avant l'émission de la facture qui devra être envoyée sur la plateforme CHORUS.

2.6 Renseignements

Pour obtenir tous renseignements complémentaires qui leur seraient nécessaires au cours de leur étude, les candidats devront passer prioritairement par la plateforme marchés publics PLACE (<http://www.marches-publics.gouv.fr>)

3 Lot 1 : Accompagnement au système de management intégré (SMI)

3.1 Besoin

Ce premier lot concerne l'accompagnement sur mesure pour le maintien en conformité et l'amélioration du SMI du GRADeS, incluant son adaptation aux évolutions futures des référentiels ISO 9001:2015, ISO 27001:2022 et de la certification Hébergeur de Données de Santé (HDS)

3.1.1 Périmètre des prestations

Le périmètre des prestations couvre l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à garantir le fonctionnement du SMI du GRADeS BFC ainsi que les processus métiers associés.

Les prestations attendues peuvent être (Liste non exhaustive) :

- La mise en œuvre de la politique de sécurité
- Formalisation de politiques spécifiques
- Formalisation de procédures opérationnelles
- L'intégration de la sécurité dans les projets
- La constitution de modalités de pilotage de la sécurité des SI (tableaux de bord, suivi d'audit...)
- L'accompagnement dans la gestion de crise
- La réalisation d'exercice de crise
- L'analyse et la gestion des risques
- La conformité méthodologique et normative
- La définition des bonnes pratiques (ITIL...)
- La définition des niveaux de services de sécurité (SLA...)
- Tout processus en lien avec la Sécurité des Systèmes d'Information

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

Attention : Les zones entourées de crochets [] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

Erreur ! Source du renvoi introuvable.

3.1.2 Cas d'usage pour l'analyse des offres

Afin d'apprécier la compréhension du besoin par les candidats ainsi que la pertinence de leur approche méthodologique, le GRADeS BFC demande aux candidats de décrire, dans leur offre, la manière dont ils traiteraient les cas d'usage ci-dessous.

Les réponses attendues portent principalement sur la méthodologie proposée, l'organisation de la mission, les compétences mobilisées et les livrables envisagés.

Les candidats ne sont pas tenus de produire les livrables complets mais devront présenter leur approche et les principales étapes de leur intervention, ainsi que le nombre de jours associés tant côté fournisseur que côté GRADeS BFC.

- Cas d'usage n°1 : Evolution de la veille sur la gestion des menaces

Le GRADeS BFC souhaite renforcer son dispositif de veille relative aux menaces susceptibles d'affecter la sécurité de ses systèmes d'information, conformément aux recommandations du contrôle 5.7 de la norme ISO/IEC 27002:2022

Le candidat décrira :

- Les sources d'information pertinentes susceptibles d'être exploitées
- Les modalités de collecte, d'analyse et de qualification des informations relatives aux menaces
- L'organisation du processus de veille (rôles et responsabilités, fréquence d'analyse, modalités de diffusion de l'information)
- La manière dont les informations collectées seraient intégrées dans les processus existants, notamment la gestion des risques SSI, les processus de gouvernance du SMI
- Les livrables et supports susceptibles d'être produits (bulletins de veille, tableaux de bord, synthèses pour la gouvernance, etc.)
- Les indicateurs permettant d'évaluer l'efficacité du dispositif
- La charge estimée associée

- Cas d'usage n°2 : Evolution de la gestion des fournisseurs

Le GRADeS BFC souhaite faire évoluer son processus de gestion des fournisseurs afin de renforcer :

- La maîtrise des prestations externalisées
- La prise en compte des enjeux de sécurité de l'information
- L'alignement avec les exigences des référentiels ISO 9001:2015 et ISO 27001:2022

Le candidat décrira :

- La méthodologie permettant d'analyser l'existant et d'identifier les axes d'amélioration du

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

Attention : Les zones entourées de crochets [] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

Erreur ! Source du renvoi introuvable.

processus de gestion des fournisseurs

- Les modalités de prise en compte des exigences des référentiels ISO 9001 et ISO 27001, notamment en matière d'évaluation des fournisseurs, de gestion des risques liés aux tiers, de suivi des performances des prestataires
- Les mécanismes permettant d'assurer la prise en compte des exigences de sécurité de l'information dans les relations fournisseurs
- Les propositions relatives à la formalisation du processus, aux outils de suivi et aux indicateurs de pilotage
- Les modalités de suivi et de réévaluation des fournisseurs
- Les livrables susceptibles d'être produits (cartographie des fournisseurs, matrice d'évaluation, procédure de gestion des fournisseurs, etc.)
- La charge estimée associée

○ Cas d'usage n°3 : Organisation d'un exercice de gestion de crise cyber

Le GRADeS BFC souhaite organiser un exercice de gestion de crise portant sur un scénario de cyberattaque impactant un service hébergeant des données de santé

Le candidat décrira :

- La méthodologie proposée pour préparer l'exercice
- La construction du scénario
- Les acteurs impliqués
- Les modalités d'animation de l'exercice
- Les livrables produits (retour d'expérience, plan d'amélioration...)
- La charge estimée associée

○ Cas d'usage n°4 : Amélioration du pilotage du SMI

Le GRADeS BFC souhaite améliorer le pilotage de son système de management intégré.

Le candidat décrira :

- Les indicateurs qu'il recommanderait pour piloter un SMI couvrant ISO 9001, ISO 27001 et HDS
- Les modalités de suivi proposées
- La comitologie associée
- Les outils ou méthodes permettant d'améliorer la lisibilité des tableaux de bord
- La charge estimée associée

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

Attention : Les zones entourées de crochets [] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

Erreur ! Source du renvoi introuvable.

3.2 Suivi et Evaluation

Afin d'assurer le pilotage, le suivi et l'évaluation des prestations réalisées dans le cadre du présent marché, des comités de suivi seront organisés entre l'organisation et le prestataire.

Ces comités ont pour objectif de permettre un échange régulier sur l'avancement des travaux, les orientations à privilégier, les éventuelles difficultés rencontrées ainsi que les actions correctives ou d'amélioration à mettre en œuvre. Ils constituent également un cadre de dialogue permettant d'évaluer la qualité des prestations réalisées et d'identifier les besoins d'évolution ou d'adaptation des interventions.

A minima, un comité devra être organisé une fois par an sur la durée du marché. Ce comité permettra notamment de réaliser un bilan des prestations réalisées, d'évaluer la pertinence des actions menées au regard des objectifs du marché et de définir les axes d'amélioration ou les priorités pour la période suivante.

Le prestataire est toutefois libre de proposer une organisation de gouvernance reposant sur une périodicité différente ou complémentaire, s'il estime qu'une fréquence de comités plus régulière est de nature à améliorer la qualité du pilotage, la réactivité dans le traitement des sujets ou l'efficacité globale des prestations.

Dans ce cas, le prestataire devra justifier dans son offre la périodicité proposée, en précisant les objectifs poursuivis, les modalités d'organisation des comités (type de comité, participants, livrables attendus, modalités de restitution) ainsi que la valeur ajoutée apportée par cette organisation au regard des enjeux du marché et des besoins de l'organisation.

Le prestataire donnera la charge associée à ce suivi.

3.3 Capacités individuelles exigées

Le candidat devra décrire dans son offre l'organisation et la composition de son équipe pour répondre aux attentes du GRADeS BFC.

Il s'agit d'apprécier notamment la pertinence de l'équipe dédiée proposée, des profils additionnels et de son organisation.

Le candidat fournira les CVs (non anonymes) des intervenants affectés à l'exécution de la mission, de la date de notification du marché jusqu'à la fin du marché.

Pour chaque intervenant et remplaçant proposé, il sera présenté :

- Ses références sur des missions similaires
- Les résultats atteints
- En quoi ses compétences acquises conviennent à l'exécution de la mission objet du présent marché et à son succès

Les compétences des intervenants devront notamment couvrir les référentiels et méthodes suivants :

- ISO 27001 Lead Auditor

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

Attention : Les zones entourées de crochets [] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

Erreur ! Source du renvoi introuvable.

- ISO 27001 Implementor
- ISO 27005
- Ebios RM
- ISO 9001
- ISO 20000
- ITIL
- RGPD

Les intervenants présentés dans l'offre sont réputés constituer l'équipe dédiée à l'exécution des prestations. Le candidat précisera dans son offre le rôle exact de chaque intervenant, son niveau d'implication dans les différentes prestations ainsi que le volume estimé de jours d'intervention sur la durée du marché.

Une attention particulière sera portée à la cohérence entre les profils proposés, leur niveau d'expertise et leur implication réelle dans l'exécution des missions

Le titulaire s'engage à mobiliser les profils proposés dans son offre pendant toute la durée du marché.

Tout remplacement d'un intervenant devra faire l'objet d'une validation préalable du GRADeS BFC. Le remplaçant devra présenter un niveau de compétence et d'expérience au moins équivalent à celui de l'intervenant initialement proposé.

3.4 Références Clients

Le candidat devra disposer :

- D'un historique de missions réalisées pour au moins un organisme du secteur de la santé
- D'auditeurs qualifiés ou expérimentés dans la réalisation d'audits sur les référentiels suivants sur les référentiels ISO9001, ISO27001, ISO27701, ISO20000-1 & HDS avec au moins 5 Ans d'expérience

Il pourra accompagner sa réponse d'étude de cas précédemment réalisées.

3.5 Références groupes de travail spécialisés

Il sera attendu du candidat de :

- Disposer de références au sein de groupes de travail spécialisés (Notamment ISO, ou Afnor Normalisation)
- Justifier la participation à des conférences et colloques d'experts de la cybersécurité (exemple : IHEDN, Colloques auditeurs AFNOR, FIC, NUMEUM, etc).

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

Attention : Les zones entourées de crochets [] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

Erreur ! Source du renvoi introuvable.

4 Lot 2 : Audit Interne

4.1 Besoin

Dans le cadre de sa politique d'audit Interne, le GRADeS a décidé d'auditer annuellement l'ensemble du périmètre de son SMI.

Le périmètre du SMI comprend à date :

- 13 processus qualité
- 2 sites physiques (Besançon et Chalon sur Saône)
- 87 collaborateurs

Ce périmètre est susceptible d'évoluer tout au long de la durée du marché.

Il s'agira ici de proposer une prestation d'audit interne du système de management intégré selon les exigences de l'ISO 27001, ISO 9001 et HDS en simultané et ceci afin de :

- S'assurer de :
 - La conformité des pratiques par rapport aux politiques et procédures définies
 - L'efficacité du SMI
- Identifier les actions correctives nécessaires
- Améliorer le SMI

Le candidat devra détailler la méthodologie qu'il propose pour mener ces audits.

Il détaillera notamment :

- Le nombre de jours relatifs à l'audit documentaire
- Le nombre de jours relatifs à l'audit sur site
- L'ordre du jour des réunions de Lancement et de clôture

Le candidat proposera un exemple de plan d'audit.

Le candidat pourra également proposer en option une prestation d'audit sur le volet RGPD.

4.2 Exigences Normatives

Le prestataire devra respecter les exigences normatives suivantes pour auditer le SMI du GRADeS :

- Norme ISO 27001 :2022
- Référentiel HDS version2
- Norme ISO 9001 :2015

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

Attention : Les zones entourées de crochets [] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

Erreur ! Source du renvoi introuvable.

4.3 Exigences compétences / expertises

Le personnel du prestataire devra justifier des compétences et/ou niveau d'expertise suivants :

- Certification ISO27001 :2022 Lead Auditor
- Formation ISO 9001:2015 Lead Auditor

Et/ou

- Justifier d'une expérience de 5 ans a minima dans l'exécution de missions d'audit SMI

Le candidat fournira les CVs (non anonymes) des intervenants affectés à l'exécution de la mission et les copies des certificats des collaborateurs.

4.4 Définitions à utiliser

Ci-après la liste des définitions qui devront être utilisées lors des audits.

4.4.1 Point fort (PF) :

Élément du Système de Management conforme aux exigences du référentiel sur lequel l'organisme se distingue par une pratique, méthode ou technique jugée particulièrement performante.

4.4.2 Piste de Progrès (PP) :

Voie identifiée sur laquelle l'organisme peut progresser. La Piste de Progrès donne à l'organisme Client la possibilité d'améliorer la performance d'un ou plusieurs éléments de son Système de Management.

4.4.3 Point Sensible (PS) ou Point de Vigilance (PV) :

Élément du SM sur lequel des preuves d'audit montrent que l'organisme risque de ne plus satisfaire aux exigences du référentiel à court ou moyen terme. D'une manière générale cet élément affecte la performance du SM.

Un PS ou PV selon le type de prestation étant un constat particulier par rapport au référentiel d'audit :

- Son libellé ne doit pas prêter à confusion
- Sous certaines conditions, l'Instance de décision peut le requalifier en non-conformité majeure ou en non-conformité mineure
- Il doit être réévalué à l'audit suivant

POINT IMPORTANT : il est demandé de préciser pour chaque PS ou PV identifié, le risque associé afin de justifier le classement.

Un PS ou un PV ne donne pas lieu systématiquement à une action corrective mais doit être pris en compte par l'organisme.

4.4.4 Non-conformité Mineure (NC. Min.)

Non-satisfaction d'une exigence spécifiée ne compromettant pas à elle seule l'efficacité ou l'amélioration du Système de Management. Une certification peut sur recommandation du RA être délivrée, maintenue ou renouvelée en présence de Non-conformités mineures non levées.

Un ensemble de Non-Conformités Mineures non levées peut être considéré par l'Instance de Décision comme constituant globalement une Non-Conformité Majeure.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

Attention : Les zones entourées de crochets [] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

Erreur ! Source du renvoi introuvable.

Toute non-conformité mineure doit faire l'objet d'une action corrective

4.4.5 Non-conformité Majeure (NC. Maj.)

Non-satisfaction d'une exigence du référentiel touchant l'organisation, l'application ou la formalisation du Système de Management et entraînant un risque avéré (c'est-à-dire fondé sur des éléments objectifs) de non-respect, récurrent ou unique en cas le risque très important, d'une exigence spécifiée.

Non-satisfaction d'une exigence mettant en cause le fonctionnement, l'efficacité ou l'amélioration du Système de Management.

Toute non-conformité majeure doit faire l'objet d'une action corrective. Une certification ne peut être délivrée, maintenue ou renouvelée tant qu'il reste une Non-Conformité Majeure non levée

4.4.6 Note :

Constat de conformité par rapport au référentiel d'audit.

Une note est utilisée pour :

- Garder trace d'un constat effectué lors de l'audit et documenté dans le rapport et/ou assurant
- Que la partie d'audit a bien été évaluée sans qualificatif particulier
- Répondre aux « points spécifiques à auditer » prévus lors de la Revue préparatoire
- Préciser une spécificité notable du Système de Management

4.5 Plan d'audit

Le plan d'audit devra respecter le formalisme suivant :

Date / Heure	Préciser les noms des sites audités et des processus/services du référentiel, concernés (*)	§ ISO 9001	§ ISO 27001	§ HDS	Equipe d'audit	Audités - Personnes et Fonctions
Indiquer le Jour et le site concerné (Exemple : Mardi 22 Novembre 2022 - BESANCON)						
Date et créneau horaire	Exemple : <u>Support et gestion des incidents de sécurité</u> - Support Clients et interne (volet SI) et gestion des incidents : organisation, procédures, lien avec la gestion des incidents de sécurité ; - Gestion des incidents de sécurité : définitions, procédures, audit de cas ; - Exigences HDS (et RGPD) : traitement des violations de DSCP.		Exemple : A.16	Exemple : 4.4.5.1	Exemple : RA	Lister les personnes allant être auditées (Prénom, Nom et Fonction)

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

Attention : Les zones entourées de crochets [] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

Erreur ! Source du renvoi introuvable.

4.6 Fiches de non-conformité.

Les fiches de non-conformité issues des audits devront avoir à minima les items suivants :

- Référence de la NC :
- Type de non-conformité : ☐ Majeure ☐ Mineure
- Date de constat de la NC : JJ/MM/AAAA
- Auditeur(s) : Prénom Nom (Société)
- DESCRIPTION DE LA NON-CONFORMITÉ
 - Rappel de l'exigence (référence...) et Extrait
 - (Exemple : NF EN ISO/IEC 27001 :2017 - 6.2 - Objectifs de sécurité de l'information et plans pour les atteindre)
 - Constat(s) relevé(s)
 - Libellé/détail de la non-conformité
 - Risque (client/produit/processus/système)

Le candidat proposera un exemple de fiche de non-conformité.

4.7 Propositions d'actions

Pour chaque écart relevé (Non-conformité de tout type, PS ou PP) le candidat proposera des actions correctives et /ou préventives afin de corriger l'écart.

4.8 Références Clients

Le candidat devra disposer :

- D'un historique de missions réalisées pour au moins un organisme du secteur de la santé
- D'auditeurs qualifiés ou expérimentés dans la réalisation d'audits sur les référentiels suivants sur les référentiels ISO9001, ISO27001, ISO27701, ISO20000-1 & HDS avec au moins 5 Ans d'expérience

Il pourra accompagner sa réponse d'étude de cas précédemment réalisées.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

Attention : Les zones entourées de crochets [] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

Erreur ! Source du renvoi introuvable.

5 Lot 3 : Accompagnement juridique et réglementaire en lien avec l'intelligence artificielle, les technologies innovantes et le SMI et Règlementaire

5.1 Besoin

Dans le cadre de ses activités, le GRADeS est tenu de :

- Maîtriser les cadres normatifs, législatifs et réglementaires régissant le numérique en santé, notamment face à l'essor de l'intelligence artificielle et des technologies émergentes
- Maintenir une veille légale et réglementaire permanente, garantissant la conformité de son système de management intégré (SMI)

Pour répondre à ces exigences, le GRADeS recherche un prestataire en mesure de :

- Lui fournir une veille légale et réglementaire exhaustive et régulièrement mise à jour, couvrant les domaines prioritaires :
 - La cybersécurité et la gouvernance des systèmes d'information
 - La protection et la gestion des données à caractère personnel
 - L'innovation numérique en santé et les nouvelles technologies

5.2 Accompagnement juridique et réglementaire

Dans le cadre de ses activités, le GRADeS BFC sollicite un prestataire capable de fournir un accompagnement juridique et réglementaire opérationnel, couvrant à minima les domaines suivants :

- **L'appui à la structuration et à l'amélioration des processus internes** au regard des exigences légales et réglementaires applicables au secteur de la santé numérique mais également des besoins métiers et des évolutions identifiées lors de la veille.
- **Cadrage juridique de sujet de différentes natures (projets/POC/expérimentation scientifique/AAP..)** variants les périmètres, acteurs et thématique : accompagnement juridique en amont et tout au long de projets numériques en santé, y compris les projets innovants impliquant des technologies émergentes (dont l'intelligence artificielle et DM sur la qualification du risque SIA et DM), afin d'en sécuriser les aspects légaux, réglementaires et contractuels dès la phase de pré-qualification.
- **L'aide et support à la production et révision documentaire spécifique** sur des documents tel que :
 - Analyses d'impact relatives à la protection des données (AIPD)
 - Convention d'hébergement, de convention de partage de données de santé et autres documents associées
 - Contrats d'utilisation de solutions (éditeurs, intégrateurs, partenaires)
 - Accords de confidentialité

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

Attention : Les zones entourées de crochets [] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

Erreur ! Source du renvoi introuvable.

- Conditions générales d'utilisation (CGU)
- [...]
- **Appui juridique lors de certaines réunions en tant qu'expert** pour accompagner le GRADeS sur certains sujet (ex : échange avec des fournisseurs, réunion avec différents acteurs...) mais également lors de besoin d'expertise ciblée et ponctuelle interne aux activités du GRADeS.

Cas d'usage n°1: Accompagnement à la mise en conformité RIA et structuration de la gouvernance des systèmes d'IA en santé

Le GRADeS souhaite, dans le cadre de l'entrée en application du Règlement Européen sur l'Intelligence Artificielle (RIA), structurer une gouvernance et un processus permettant de garantir la conformité des systèmes d'IA utilisés ou déployés dans le champ de la santé numérique.

Le candidat décrira :

- La méthodologie d'analyse de l'existant permettant d'identifier les usages d'IA, les processus associés et les écarts au regard des exigences du RIA (cartographie, qualification des cas d'usage et des niveaux de risque)
- Les modalités de mise en place d'une gouvernance IA (rôles et responsabilités : pilotage, métiers, juridique, sécurité)
- Les mécanismes permettant d'assurer la prise en compte des exigences du RIA (transparence, garantie humaine, gestion des risques, qualité des données, traçabilité)
- Les propositions relatives à la formalisation du processus général
- Les livrables produits
- La charge estimée associée à la mise en œuvre de la démarche

5.3 Veille légale et réglementaire

Afin de garantir au GRADeS une connaissance toujours à jour **de la législation et la réglementation en lien avec les activités du GRADeS ainsi que ces bonnes applications, il est attendu à minima :**

- D'effectuer un suivi des évolutions législatives, réglementaires et normatives applicables à la santé numérique, à la protection des données personnelles, à la sécurité de l'information, à l'hébergement de données de santé et aux certifications associées, ainsi qu'au domaine de l'intelligence artificielle et l'innovation numérique en santé mais également sur tout ce qui concerne l'actualités autour des mêmes sujets
- Communiquer les résultats de la veille aux parties prenantes concernées de manière claire et facilement intelligible à travers un livrable. Il est noté que le GRADeS pourra solliciter le prestataire à la demande afin de pouvoir questionner ce dernier sur le rapport dans le cas ou des informations complémentaires seraient nécessaires
- Analyser les nouvelles dispositions et en évaluer les impacts

Le candidat détaillera dans son offre la méthodologie employée pour assurer cette veille et la périodicité proposée pour la remise des livrables. Le prestataire devra utiliser des sources d'informations fiables et à jour.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

Attention : Les zones entourées de crochets [] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

Erreur ! Source du renvoi introuvable.

Le candidat est invité à joindre à son dossier de réponse ses modèles de livrables de veille (il précisera le format de ces restitutions) qui seront évalués et qui devront être utilisés avec ou non adaptation du client si la prestation était retenue.

Cas d'usage n°2: Veille réglementaire, normative et innovation en santé numérique (dont la thématique IA)

Le GRADeS souhaite disposer d'une veille structurée sur les évolutions législatives, réglementaires, normatives et technologiques impactant la santé numérique, la protection des données, l'hébergement de données de santé et les nouvelles technologies dont l'intelligence artificielle.

Le candidat décrira :

- Les sources d'information exploitées
- Les modalités de collecte, d'analyse et de qualification des informations
- L'organisation du processus de veille (rôles, fréquence de collecte et d'analyse, modalités de diffusion)
- Les livrables et supports produits
- La charge estimée associée

5.4 Compétences / Expériences

Le candidat devra justifier des capacités suivantes :

Références sectorielles, au moins une expérience similaire :

- Auprès d'un organisme ou établissement du secteur de la santé
- Auprès d'une structure du secteur du numérique et/ou de la donnée

Expertises spécifiques :

- Avoir une expertise reconnue dans le domaine de la sécurité de l'information et de la protection des données personnelles
- Des connaissances spécifiques seraient appréciées concernant les modèles de référence CNIL (MR004), protocole de recherche en santé, entrepôt de données de santé, intelligence artificielle et dispositifs médicaux

Expériences attendues :

- Avoir une expérience de la mise en œuvre de veille légale et réglementaire dans le domaine du numérique, protection des données personnelles et les spécificités de la donnée de santé et son hébergement, de l'innovation en santé (notamment IA)
- Justifier de participation à des conférences et colloques d'experts du numérique en santé, de la donnée et de l'innovation numérique

Le candidat est invité à joindre à son dossier de réponse tout étude de cas ou retour d'expérience illustrant des missions antérieures jugées pertinentes au regard de l'objet du marché.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

Attention : Les zones entourées de crochets [] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

Erreur ! Source du renvoi introuvable.

Une attention particulière sera portée également à la capacité à vulgariser des sujets juridiques complexes pour une bonne compréhension et mise en application par le GRADeS.

Le candidat fournira les CVs (non anonymes).

5.5 Suivi et Evaluation

Afin d'assurer le pilotage, le suivi et l'évaluation des prestations réalisées dans le cadre du présent marché, des comités de suivi seront organisés entre l'organisation et le prestataire.

Ces comités ont pour objectif de permettre un échange régulier sur l'avancement des travaux, les orientations à privilégier, les éventuelles difficultés rencontrées ainsi que les actions correctives ou d'amélioration à mettre en œuvre. Ils constituent également un cadre de dialogue permettant d'évaluer la qualité des prestations réalisées et d'identifier les besoins d'évolution ou d'adaptation des interventions.

A minima, un comité devra être organisé une fois par an sur la durée du marché. Ce comité permettra notamment de réaliser un bilan des prestations réalisées, d'évaluer la pertinence des actions menées au regard des objectifs du marché et de définir les axes d'amélioration ou les priorités pour la période suivante.

Le prestataire est toutefois libre de proposer une organisation de gouvernance reposant sur une périodicité différente ou complémentaire, s'il estime qu'une fréquence de comités plus régulière est de nature à améliorer la qualité du pilotage, la réactivité dans le traitement des sujets ou l'efficacité globale des prestations.

Dans ce cas, le prestataire devra justifier dans son offre la périodicité proposée, en précisant les objectifs poursuivis, les modalités d'organisation des comités (type de comité, participants, livrables attendus, modalités de restitution) ainsi que la valeur ajoutée apportée par cette organisation au regard des enjeux du marché et des besoins de l'organisation.

Le prestataire donnera la charge associée à ce suivi.

6 Lot 4 : Accompagnement juridique et réglementaire spécifiques aux règles de la fonction publique

6.1 Besoin

Dans le cadre de ses activités, le GRADeS est tenu de garantir le respect de l'application des règles normatives, législatives et réglementaires incombant au GRADeS BFC afin d'assurer le bon fonctionnement du Groupement d'intérêt public

Pour répondre à ces exigences, le GRADeS recherche un prestataire en mesure de lui assurer une assistance juridique sur :

- Des prestations en justice
- Des prestations de consultation juridique
- Des prestations relatives à l'information à caractère documentaire

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

Attention : Les zones entourées de crochets [] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

Erreur ! Source du renvoi introuvable.

6.2 Assistance juridique

Afin de garantir le bon fonctionnement du GRADeS BFC, il est attendu du candidat :

- De le représenter en justice dans le cadre d'un contentieux afin d'assurer la défense de ses intérêts
- D'apporter une prestation intellectuelle relative à une consultation juridique dans les domaines recouvrant le droit de la fonction publique et en particulier le droit de la fonction publique d'Etat. Celle-ci tend à fournir un avis concourant, par les éléments qu'il apporte, à la prise de décision du GRADeS BFC
- Des prestations relatives à l'information à caractère documentaire afin de renseigner le GRADeS BFC sur l'état du droit ou de la jurisprudence relativement à un problème donné

6.3 Compétences / Expériences

Le candidat devra justifier de référence d'application et de missions auprès d'organismes publics d'Etat et en particulier Groupement d'Intérêt Public (GIP).

Le candidat devra justifier d'une ou plusieurs représentations en justice d'un organisme public d'Etat.

Le candidat fournira les CVs (non anonymes) des intervenants affectés à l'exécution de la mission et les copies des certificats des collaborateurs.

Le titulaire devra démontrer une expertise confirmée dans les domaines juridiques concernés ainsi qu'une capacité à assurer un accompagnement réactif, sécurisé et opérationnel.

Les candidats devront présenter des références comparables, les moyens humains affectés au marché, leur méthodologie d'intervention ainsi que les modalités de suivi et de reporting proposées.

***** Fin du Document *****

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

Attention : Les zones entourées de crochets [] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

Erreur ! Source du renvoi introuvable.