CAIH

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES

LOT 4

SÉCURITÉ RÉSEAU, MAINTENANCE ET SERVICES ASSOCIÉS « AVANCÉ »

Accord-cadre relatif aux infrastructures réseaux et services associés

Version 2026

Table des matières

7. Lot 4 - Sécurité réseau Avancé 3

7.1. Objet du lot 3

7.2 Règle de référencement et cadre de réponse technique 4

7.3 Index des exigences et des prix spécifiques 4

7.4 Solutions à garanties renforcées de souveraineté et de résilience 4

7.4.1 Objet 4

7.4.2 Définition applicable au présent marché 5

7.4.3 Continuité de fonctionnement en situation de restriction 6

7.4.4 Absence de mécanisme de neutralisation distante 7

7.4.5 Identification et maîtrise des dépendances critiques 7

7.4.6 Changement de contrôle, acquisition ou restructuration 8

7.4.7 Perte de la qualification en cours de marché 9

7.4.8 Présentation par domaine fonctionnel 9

7.4.9 Absence de solution souveraine conforme 10

7.4.10 Alternative informative de niveau inférieur 10

7.4.11 Justificatifs fournis sans surcoût 10

7.4.12 Tarification 11

7.5 Engagement renforcé de temps d'intervention à distance 11

7.6 Gouvernance et reporting à fréquence renforcée 12

Modalités techniques attendues 12

Livrables attendus 12

7.7 Transparence de la chaîne logicielle, des dépendances et des vulnérabilités 12

7.7.1 Informations attendues 13

7.7.2 Diligences attendues 13

7.7.3 Information relative aux vulnérabilités 13

7.7.4 Finalité de l'exigence 13

7.7.5 Prestations personnalisées 13

7.8 Réversibilité avancée 14

Modalités techniques attendues 14

Livrables attendus 14

Référence de prix 14

7.9 Cohérence avec les pièces du marché 14

7. Lot 4 - Sécurité réseau Avancé

7.1. Objet du lot

Le Lot 4 « Sécurité réseau Avancé » s'adresse aux bénéficiaires exploitant des infrastructures de sécurité critiques, multisites, fortement exposées ou soumises à des exigences renforcées de continuité, de maîtrise des risques, de souveraineté, de transparence, de réversibilité et d'expertise en sécurité réseau.

Une offre au Lot 4 comprend obligatoirement l'intégralité du socle technique, fonctionnel et tarifaire du Lot 3 « Sécurité réseau Essentiel », auquel s'ajoutent les exigences complémentaires et les engagements renforcés définis dans le présent CCTP.

À ce titre, l'ensemble des équipements, logiciels, licences, abonnements, accessoires, prestations, unités d'œuvre, services d'installation, d'intégration, de migration, de configuration, d'exploitation, de support, de maintien en condition opérationnelle et de maintien en condition de sécurité, ainsi que les obligations documentaires, de formation, de transfert de compétences et de réversibilité prévues au Lot 3, s'appliquent intégralement au Lot 4.

Les solutions du Lot 4 doivent donc satisfaire, sans réduction ni substitution, à toutes les exigences communes et à toutes les exigences propres au Lot 3, sauf disposition contraire expressément prévue par le présent CCTP pour les exigences complémentaires SEC-ADV.

En complément de ce socle, le Lot 4 impose, pour les domaines fonctionnels de sécurité réseau concernés, la proposition d'au moins une solution à garanties renforcées de souveraineté et de résilience lorsqu'une telle solution existe et répond aux besoins techniques. Cette exigence comprend notamment la maîtrise des opérations essentielles depuis l'Union européenne, la localisation et la maîtrise des données, journaux, configurations et services critiques, la continuité de fonctionnement en cas d'indisponibilité de services externes, l'absence de neutralisation distante non maîtrisée, l'identification des dépendances techniques, juridiques, capitalistiques et opérationnelles, ainsi que le maintien et l'actualisation de la qualification pendant toute la durée du marché.

Le Lot 4 impose également, pour les équipements, logiciels et services identifiés comme critiques dans le bon de commande, une garantie de temps d'intervention à distance de trente (30) minutes maximum, vingt-quatre heures sur vingt-quatre et sept jours sur sept. Cette GTI renforcée est obligatoire. Une GTR renforcée, notamment de deux (2) heures H24/7, peut être proposée et valorisée par le candidat, mais ne constitue pas une exigence minimale du Lot 4. Sauf indication explicite contraire, les définitions, modalités de calcul, exclusions, suspensions de délais, conditions de clôture, engagements d'intervention physique, reporting et pénalités demeurent ceux du CCTP commun.

La gouvernance et le reporting sont renforcés : un comité de suivi et un reporting consolidé d'activité, de maintenance, de vulnérabilités et de niveaux de service sont organisés au minimum chaque trimestre, en remplacement de la fréquence semestrielle du socle commun. Le reporting est remis dans les quinze jours suivant la période concernée et couvre notamment l'activité, les incidents, le respect des SLA, la maintenance préventive, les versions et correctifs, les vulnérabilités affectant les solutions, les écarts, les risques et les plans d'action. La fréquence est adaptée sans délai en cas d'incident majeur, de vulnérabilité critique, de dérive de niveau de service ou de risque significatif, et chaque réunion donne lieu à un compte rendu, un relevé de décisions, un plan d'action, des responsables désignés et des échéances de suivi.

Le titulaire doit en outre assurer une transparence renforcée de la chaîne logicielle, des dépendances et des vulnérabilités : informations relatives aux composants majeurs, versions, cycles de maintenance, dates de fin de support, dépendances techniques ou services externes, vulnérabilités affectant les solutions, procédures de mise à jour, de correction et de remédiation, ainsi que nomenclature logicielle ou document équivalent lorsqu'il existe et est accessible au titulaire. Cette exigence constitue une obligation de moyens renforcée et ne donne pas lieu à une tarification spécifique.

Enfin, le Lot 4 ajoute une réversibilité avancée couvrant la restitution des configurations, sauvegardes, inventaires, licences, schémas, matrices de flux, politiques de sécurité, règles, objets, certificats et procédures, l'export des données d'administration, de supervision, des journaux et des référentiels dans des formats exploitables, la restitution ou la suppression contrôlée des accès, comptes, certificats, secrets et moyens de télémaintenance,

ainsi que l'assistance à la reprise, le transfert de connaissances et l'accompagnement du tiers repreneur. Ce complément est décrit, justifié et, lorsque prévu, valorisé au moyen des références tarifaires spécifiques du Lot 4, sans duplication ni double facturation des prestations déjà comprises dans le Lot 3. En cas de contradiction, le présent CCTP prévaut uniquement pour ces exigences complémentaires ou renforcées.

RÈGLE D'ARTICULATION : le candidat répond au socle complet du Lot 3 et aux seules exigences supplémentaires du Lot 4. Il identifie clairement les engagements et prix propres au niveau Avancé, sans dupliquer ni modifier les exigences de maintenance communes.

7.2 Règle de référencement et cadre de réponse technique

Chaque exigence structurante propre au Lot 4 est identifiée par le préfixe SEC-ADV suivi d'un numéro séquentiel. Le candidat reprend cette référence dans le CRT et ses justificatifs. Il indique le niveau de conformité, la réponse détaillée, les prérequis, dépendances, limites, réserves et preuves documentaires.

Référence CCTP	Domaine	Réponse du candidat	Conformité	Justificatif	Limites
SEC-ADV-XXX	Lot 4	Réponse détaillée et opposable	Conforme / Partiellement conforme / Non conforme	Document, page et section	Écarts, prérequis, exclusions

7.3 Index des exigences et des prix spécifiques

Exigence	Objet	Traitement tarifaire
SEC-ADV-001	Solutions à garanties renforcées de souveraineté et de résilience	Caractéristique qualifiante preuves incluses sans surcoût
SEC-ADV-020	Gouvernance et reporting renforcés	Inclus dans les prix du Lot 4
SEC-ADV-030	GTI à distance renforcée	Incluse pour les périmètres critiques commandés
SEC-ADV-040	Transparence de la chaîne logicielle, des dépendances et des vulnérabilités	Exigence intrinsèque informations et mises à jour incluses sans surcoût
SEC-ADV-050	Réversibilité avancée	P4805 - forfait par périmètre technique

7.4 Solutions à garanties renforcées de souveraineté et de résilience

7.4.1 Objet

[SEC-ADV-001] Pour chacun des domaines fonctionnels définis dans le CCTP du Lot 3, le candidat propose, lorsqu'elle existe, au moins une solution répondant à la définition de la solution à garanties renforcées de souveraineté établie par le présent article et satisfaisant aux exigences techniques, fonctionnelles, de capacité et de performance applicables au domaine et à la gamme concernés.

L'objectif est de permettre aux bénéficiaires de disposer de solutions dont l'exploitation, l'administration, la supervision, la sécurité, la maintenance et la pérennité ne peuvent pas être interrompues ou significativement dégradées du seul fait :

- d'une décision prise par un État tiers à l'Union européenne
- de l'application d'une législation étrangère à portée extraterritoriale
- d'une mesure de sanction, d'embargo, de restriction commerciale ou de contrôle des exportations
- de l'interruption d'un service technique, commercial ou numérique opéré depuis un État tiers
- d'une décision unilatérale de l'éditeur, du constructeur, d'un fournisseur cloud ou d'un autre prestataire critique
- d'un changement de contrôle, d'une fusion, d'une acquisition ou d'un transfert d'activité affectant l'éditeur, le constructeur ou un prestataire critique.

La présente exigence porte sur les caractéristiques intrinsèques de la solution et sur les conditions durables de son exploitation. Elle ne constitue pas une prestation documentaire autonome.

Les informations, déclarations et justificatifs nécessaires à l'évaluation de la solution sont fournis nativement par le candidat, sans surcoût, dans son offre et pendant toute la durée du marché.

7.4.2 Définition applicable au présent marché

Au sens du présent marché, est qualifiée de solution à garanties renforcées de souveraineté une solution technique répondant aux exigences du Lot 3 et présentant simultanément les caractéristiques suivantes :

1. les opérations essentielles de support, de maintenance, d'administration et de supervision peuvent être assurées par le titulaire, l'éditeur, le constructeur ou leurs sous-traitants depuis l'Union européenne
2. les données, métadonnées, journaux, configurations, sauvegardes, secrets et informations d'administration peuvent être hébergés, traités, conservés et exploités au sein de l'Union européenne
3. les fonctions essentielles de sécurité, d'administration, de supervision, de journalisation, de sauvegarde et de restauration restent opérationnelles sans dépendance obligatoire à un service cloud, à une plateforme de gestion ou à une infrastructure technique située hors de l'Union européenne ou non maîtrisée par le bénéficiaire
4. la solution ne dépend pas, pour son fonctionnement essentiel, d'un mécanisme distant d'activation, de validation, d'autorisation ou de renouvellement dont l'interruption pourrait désactiver la solution, empêcher son administration ou provoquer une dégradation substantielle de ses fonctions de sécurité
5. les équipements et logiciels déjà déployés ne comportent pas de mécanisme permettant leur désactivation à distance par l'éditeur, le constructeur ou un tiers, hors action expressément autorisée par le bénéficiaire dans le cadre d'une opération de support identifiée et traçable

1. le bénéficiaire conserve la maîtrise de ses configurations, règles, politiques, journaux, sauvegardes, certificats, clés, référentiels et données nécessaires à la continuité de l'exploitation
2. la solution dispose de mécanismes documentés de sauvegarde, d'export, de restauration et de réversibilité permettant au bénéficiaire de poursuivre l'exploitation, de reprendre l'administration ou d'en transférer la gestion à un tiers
3. les conditions de licence, de souscription ou de support n'autorisent pas la désactivation immédiate des fonctions déjà acquises et déployées du seul fait d'une restriction géopolitique, commerciale ou juridique extérieure au bénéficiaire

4. la solution peut continuer à assurer ses fonctions essentielles pendant une durée suffisante en cas d'interruption des services externes nécessaires aux mises à jour, à la télémétrie, au renseignement sur les menaces, à la réputation, à la catégorisation, à l'activation ou au support
5. les dépendances techniques, juridiques, capitalistiques et opérationnelles susceptibles d'affecter la continuité de la solution sont identifiées, documentées et tenues à jour.

L'établissement d'un éditeur, d'un constructeur, du titulaire ou d'un prestataire au sein de l'Union européenne constitue un élément d'appréciation, mais ne suffit pas, à lui seul, à qualifier la solution.

La qualification prend également en compte :

- la localisation et le contrôle effectif des activités critiques
- la structure de contrôle de l'éditeur ou du constructeur
- les juridictions auxquelles les entités critiques sont soumises
- la localisation des services techniques indispensables
- les dépendances aux sociétés mères, filiales, sous-traitants, fournisseurs cloud et composants tiers
- les conséquences d'un changement de contrôle ou d'une acquisition par une entité située hors de l'Union européenne.

7.4.3 Continuité de fonctionnement en situation de restriction

Le candidat décrit, pour chaque solution proposée, les conséquences d'une interruption totale ou partielle :

- de la connexion Internet
- des services cloud de l'éditeur ou du constructeur
- des serveurs d'activation ou de validation des licences
- des services de support distants
- des services de téléchargement des correctifs et mises à jour
- des bases de signatures, de réputation, de catégorisation ou de renseignement sur les menaces
- des services de télémétrie et de supervision externe
- des plateformes d'administration centralisée
- de tout autre service externe nécessaire à l'exploitation de la solution.

Le candidat distingue clairement :

- les fonctions restant pleinement opérationnelles
- les fonctions disponibles en mode dégradé
- les fonctions devenant indisponibles
- le délai avant dégradation ou interruption
- les conséquences sur la sécurité et la continuité de service
- les modes opératoires locaux ou alternatifs disponibles
- les mesures compensatoires pouvant être appliquées par le bénéficiaire.

Une solution dont les fonctions essentielles cessent immédiatement de fonctionner en cas d'indisponibilité d'un service externe non maîtrisé ne peut pas être qualifiée de solution à garanties renforcées de souveraineté.

7.4.4 Absence de mécanisme de neutralisation distante

Le candidat indique si la solution comporte un mécanisme permettant à l'éditeur, au constructeur, au fournisseur d'un composant ou à un autre tiers :

- de désactiver tout ou partie du produit
- de suspendre une licence ou une souscription déjà activée
- d'empêcher l'accès à l'administration
- de supprimer ou de limiter une fonctionnalité
- de bloquer le démarrage ou le redémarrage
- de modifier à distance une configuration
- d'interrompre l'accès aux mises à jour ou aux données nécessaires à l'exploitation
- de rendre un équipement ou logiciel inopérant.

Lorsque de tels mécanismes existent, le candidat précise :

- leur finalité
- leurs conditions d'activation
- l'entité qui peut les déclencher
- les mesures de contrôle et de traçabilité
- la possibilité de les désactiver
- les conséquences de leur déclenchement
- les garanties contractuelles empêchant leur utilisation sans accord du bénéficiaire.

Le candidat fournit un engagement explicite indiquant qu'aucune action de désactivation, de restriction fonctionnelle ou de neutralisation à distance ne peut être engagée sans information préalable du bénéficiaire, sauf nécessité immédiate liée à la sécurité et expressément prévue par les documents contractuels.

7.4.5 Identification et maîtrise des dépendances critiques

Pour chaque solution, le candidat identifie les dépendances nécessaires :

- au fonctionnement nominal
- à l'administration
- à la supervision
- à l'activation et au renouvellement des licences
- à la sécurité
- au téléchargement des mises à jour
- à l'actualisation des signatures, moteurs, bases de réputation ou de catégorisation
- à l'accès au support
- à la sauvegarde et à la restauration
- à la continuité de service.

Pour chaque dépendance critique, le candidat précise :

- le fournisseur concerné

- sa localisation
- l'entité qui en assure le contrôle
- les juridictions applicables
- son caractère obligatoire ou facultatif
- la possibilité de la désactiver ou de la substituer
- les conséquences de son indisponibilité
- les mesures permettant de poursuivre l'exploitation.

Une dépendance située au sein de l'Union européenne mais contrôlée par une entité soumise à une juridiction extra-européenne est déclarée comme telle.

7.4.6 Changement de contrôle, acquisition ou restructuration

La qualification d'une solution à garanties renforcées de souveraineté est appréciée non seulement lors de la remise de l'offre, mais pendant toute la durée du marché.

Le titulaire informe la CAIH, dans les meilleurs délais et dès qu'il en a connaissance, de tout événement susceptible de modifier la qualification de la solution, notamment :

- changement direct ou indirect de contrôle de l'éditeur ou du constructeur
- acquisition par une entité établie hors de l'Union européenne
- fusion ou rapprochement capitalistique
- transfert d'une activité critique hors de l'Union européenne
- changement d'entité assurant le développement, la maintenance, l'administration ou le support
- modification des juridictions applicables
- ajout d'un service cloud obligatoire
- transfert de données, de journaux, de télémétrie ou d'opérations d'administration hors de l'Union européenne
- recours à un nouveau sous-traitant critique
- modification substantielle des conditions de licence, de souscription, d'activation ou de support
- perte ou modification d'une certification, qualification ou évaluation de sécurité ayant contribué à l'appréciation de la solution.

Le titulaire analyse les conséquences de cet événement et transmet à la CAIH :

- la description du changement
- les fonctions, données, services et bénéficiaires potentiellement concernés
- l'incidence sur les critères du présent article
- les mesures de continuité et de réduction du risque
- le calendrier de mise en œuvre des mesures correctives
- le cas échéant, les solutions de remplacement disponibles.

Un acteur initialement européen ne conserve donc pas automatiquement la qualification de solution à garanties renforcées de souveraineté après son acquisition ou son contrôle par une entité extra-européenne. La qualification est réévaluée au regard du contrôle effectif, des juridictions applicables, des dépendances techniques et de la continuité réelle d'exploitation.

7.4.7 Perte de la qualification en cours de marché

Lorsque l'évolution de l'éditeur, du constructeur, de la solution ou de son environnement ne permet plus de satisfaire aux exigences du présent article, le titulaire :

1. en informe la CAIH et les bénéficiaires concernés
2. cesse de présenter la solution comme une solution à garanties renforcées de souveraineté
3. identifie les risques pesant sur les solutions déjà déployées
4. précise les fonctions susceptibles d'être interrompues ou dégradées
5. propose les mesures de continuité immédiatement applicables
6. présente, lorsqu'elle existe, une solution de remplacement conforme
7. fournit les éléments nécessaires à la réversibilité et à la migration.

La perte de la qualification n'entraîne pas automatiquement l'arrêt d'utilisation de la solution par les bénéficiaires. Elle interdit en revanche de continuer à la présenter ou à la commercialiser comme répondant aux exigences de souveraineté du Lot 4.

Les conditions administratives et financières applicables à une migration rendue nécessaire par la perte de qualification, notamment lorsqu'elle résulte d'un changement imputable à l'éditeur, au constructeur ou au titulaire, sont précisées dans le CCAP.

7.4.8 Présentation par domaine fonctionnel

Pour chacun des domaines fonctionnels du Lot 3, le candidat indique :

- si une solution à garanties renforcées de souveraineté est disponible
- l'éditeur ou le constructeur
- la référence commerciale
- les gammes couvertes
- le mode de déploiement
- les références du BPU ou du catalogue
- les critères de souveraineté satisfaits
- les dépendances critiques
- le niveau d'autonomie en cas d'interruption des services externes
- les mécanismes éventuels de désactivation ou de restriction distante
- les documents probants
- les limites, écarts, prérequis et réserves.

Une même solution peut couvrir plusieurs domaines fonctionnels. Dans ce cas, la conformité est présentée séparément pour chaque domaine et chaque gamme concernés.

Le Lot 3 définit déjà les domaines fonctionnels, gammes et références tarifaires, ainsi que les informations à communiquer pour chacune des solutions proposées. La présente section complète cette qualification sans recréer les gammes ni les prix du Lot 3.

7.4.9 Absence de solution souveraine conforme

Lorsqu'aucune solution à garanties renforcées de souveraineté ne permet de satisfaire aux exigences techniques et fonctionnelles d'un domaine, le candidat l'indique explicitement dans le CRT.

Il précise alors :

- le domaine et les gammes concernés
- les solutions ou éditeurs examinés
- les critères de souveraineté non satisfaits
- les caractéristiques techniques ou fonctionnelles manquantes
- les services ou dépendances incompatibles avec le présent article
- les éventuelles évolutions annoncées par les éditeurs, en distinguant les engagements fermes des orientations non contractuelles.

L'absence de solution conforme ne constitue pas, à elle seule, une non-conformité de l'ensemble de l'offre, dès lors qu'elle est clairement déclarée et justifiée selon les modalités prévues par le présent article.

7.4.10 Alternative informative de niveau inférieur

Lorsqu'aucune solution à garanties renforcées de souveraineté ne satisfait intégralement aux exigences d'un domaine ou d'une gamme, le candidat peut présenter, à titre purement informatif, une solution présentant des caractéristiques techniques ou fonctionnelles inférieures.

Cette solution est explicitement identifiée par la mention : « Alternative souveraine informative ».

Cette alternative :

- ne se substitue pas à une solution conforme
- n'est pas comptabilisée dans le nombre minimal de solutions attendues
- ne peut pas être présentée comme répondant intégralement au CCTP
- précise les exigences satisfaites et non satisfaites
- identifie les capacités, performances ou fonctionnalités manquantes
- précise les cas d'usage plus limités auxquels elle peut néanmoins répondre
- distingue les fonctionnalités disponibles des éventuelles évolutions figurant uniquement dans une feuille de route.

7.4.11 Justificatifs fournis sans surcoût

Les informations et justificatifs permettant d'apprécier la conformité aux exigences du présent article sont fournis sans prix ni prestation complémentaire.

Ils comprennent, selon leur applicabilité :

- la structure de contrôle de l'éditeur ou du constructeur
- l'identité des entités assurant le développement, le support, la maintenance et l'administration
- la localisation des activités et infrastructures critiques

- les juridictions applicables
- la cartographie des services et dépendances externes nécessaires
- les modalités d'activation et de contrôle des licences
- les conditions de fonctionnement hors connexion ou en mode dégradé
- les mécanismes d'export, de sauvegarde, de restauration et de réversibilité
- les certifications et qualifications applicables
- les documents officiels de l'éditeur, du constructeur ou de tiers indépendants
- les engagements contractuels relatifs à la continuité et à l'absence de neutralisation distante.

Ces informations sont tenues à jour pendant toute la durée du marché sans facturation complémentaire.

Les prestations personnalisées portant sur l'environnement particulier d'un bénéficiaire, telles qu'une étude de dépendances, une cartographie locale, une architecture cible ou un plan de migration, restent commandables au moyen des lignes de services professionnels prévues dans le Lot 3. Le Lot 3 distingue déjà les preuves relatives aux solutions des audits, études, intégrations et accompagnements spécifiques assortis de livrables propres au bénéficiaire.

7.4.12 Tarification

Les solutions à garanties renforcées de souveraineté sont tarifées au moyen des lignes correspondant aux domaines, gammes, bundles, licences, abonnements, accessoires et prestations du Lot 3.

Aucune ligne tarifaire propre n'est créée pour :

- la qualification de souveraineté
- la déclaration des dépendances
- la présentation de l'actionnariat ou de la structure de contrôle
- la description du fonctionnement déconnecté ou dégradé
- les justificatifs standards
- l'actualisation des informations pendant la durée du marché
- l'information relative à un changement de contrôle ou à une perte de qualification.

La souveraineté constitue donc une caractéristique qualifiante de la solution proposée, et non un livrable facturable.

PIÈCE DE RÉPONSE : le candidat renseigne dans le CRT les critères satisfaits, les preuves, les dépendances, les limites, les modes dégradés et les éventuelles alternatives informatives.

7.5 Engagement renforcé de temps d'intervention à distance

[SEC-ADV-030] Pour les équipements, logiciels et services identifiés comme critiques dans le bon de commande, le titulaire assure une garantie de temps d'intervention (GTI) à distance de trente (30) minutes maximum, vingt-quatre heures sur vingt-quatre et sept jours sur sept, à compter de l'enregistrement de l'incident selon les modalités définies au CCTP commun.

Lorsque le diagnostic ou le rétablissement nécessite une intervention physique, le titulaire met en œuvre les moyens nécessaires selon les engagements de maintenance applicables définis au CCTP commun.

Le titulaire peut proposer des niveaux de garantie de temps de rétablissement (GTR) renforcés, notamment une GTR de deux (2) heures H24/7. Ces engagements complémentaires sont précisés dans son offre et, le cas échéant, valorisés au BPU. La proposition d'une GTR renforcée ne constitue pas une exigence minimale du lot 4.

Pour les définitions, modalités de calcul, exclusions, suspension des délais, conditions de clôture des incidents, reporting et pénalités, les dispositions du CCTP commun demeurent applicables.

7.6 Gouvernance et reporting à fréquence renforcée

[SEC-ADV-020] Les contenus, indicateurs, responsabilités et modalités de suivi applicables au Lot 3 restent inchangés. Pour le Lot 4, leur fréquence est renforcée afin de tenir compte de la criticité des infrastructures de sécurité concernées.

Modalités techniques attendues

- un comité de suivi entre le titulaire et le bénéficiaire est organisé au minimum chaque trimestre, en remplacement de la fréquence semestrielle prévue pour le socle commun
- le reporting consolidé d'activité, de maintenance, de vulnérabilités et de niveaux de service est remis au minimum chaque trimestre, dans les quinze jours suivant la période concernée
- les indicateurs comprennent notamment l'activité, les incidents, le respect des SLA, les actions de maintenance préventive, les versions et correctifs, les vulnérabilités affectant les solutions, les écarts, les risques et les plans d'action
- en cas d'incident majeur, de vulnérabilité critique, de dérive de niveau de service ou de risque significatif, la fréquence des points et reportings est adaptée à la criticité, sans attendre l'échéance trimestrielle
- chaque réunion fait l'objet d'un compte rendu, d'un relevé de décisions, d'un plan d'action, de responsables désignés et d'échéances de suivi.

Livrables attendus

N°	Livrable principal attendu
1	calendrier annuel de gouvernance
2	tableau de bord trimestriel consolidé
3	état des versions, correctifs, vulnérabilités et plans de remédiation
4	compte rendu, relevé de décisions et plan d'action mis à jour

PIÈCE DE RÉPONSE : le candidat décrit précisément son organisation, ses moyens, ses engagements, les limites éventuelles, les justificatifs associés et, lorsqu'une référence tarifaire est prévue, les éléments de prix correspondants dans le cadre de réponse technique et dans le BPU.

7.7 Transparence de la chaîne logicielle, des dépendances et des vulnérabilités

[SEC-ADV-040] Le titulaire met en œuvre tous les moyens raisonnablement accessibles, compte tenu de son rôle d'intégrateur, de distributeur ou de prestataire, afin d'obtenir, maintenir et transmettre les informations disponibles relatives à la chaîne logicielle, aux dépendances critiques, au cycle de vie et aux vulnérabilités des solutions proposées ou déployées dans le cadre du présent lot.

Cette exigence constitue une obligation de moyens renforcée. Les informations et justificatifs standards fournis au titre du présent article sont inclus dans les prix des solutions, licences, abonnements, prestations de support et de maintenance auxquels ils se rapportent. Ils ne donnent lieu à aucune tarification spécifique.

7.7.1 Informations attendues

Le titulaire fournit, dans la mesure où elles sont disponibles auprès des éditeurs, constructeurs ou fournisseurs concernés :

- les informations relatives aux composants majeurs de la solution ;
- les versions, cycles de maintenance et dates de fin de support connues ;
- les dépendances techniques ou services externes nécessaires au fonctionnement ou à l'administration ;
- les informations disponibles relatives aux vulnérabilités affectant les solutions ;
- les procédures de mise à jour, de correction et de remédiation ;
- la nomenclature logicielle (SBOM) ou tout document équivalent lorsqu'il existe et est accessible au titulaire.

7.7.2 Diligences attendues

Lorsque certaines informations ne sont pas directement disponibles, le titulaire :

- sollicite les acteurs concernés afin de les obtenir ;
- indique les informations indisponibles ;
- précise les limites connues et leurs conséquences éventuelles ;
- transmet toute information alternative pertinente dont il dispose.

L'absence de publication d'une information par l'éditeur ou le constructeur ne constitue pas, à elle seule, une non-conformité, sous réserve que le titulaire justifie les diligences raisonnablement accomplies.

7.7.3 Information relative aux vulnérabilités

Le titulaire assure une veille sur les vulnérabilités affectant les solutions qu'il fournit ou maintient. Il informe les bénéficiaires concernés de toute vulnérabilité critique ou majeure portée à sa connaissance et communique, lorsqu'ils sont disponibles :

- les versions concernées ;
- la criticité communiquée par l'éditeur ou le constructeur ;
- les correctifs disponibles ;
- les mesures compensatoires ou contournements connus.

7.7.4 Finalité de l'exigence

Les informations fournies au titre du présent article ont notamment pour objet de permettre aux bénéficiaires :

- d'apprécier les risques de sécurité associés aux solutions ;
- de mettre en œuvre leurs démarches de gestion des risques ;
- de disposer des éléments utiles à leurs obligations de cybersécurité, notamment lorsqu'ils relèvent de dispositifs tels que les opérateurs d'importance vitale (OIV), les opérateurs de services essentiels (OSE), les entités essentielles ou importantes au sens de la réglementation issue de la directive NIS2, dans sa version transposée et applicable au bénéficiaire, ou de tout dispositif équivalent.

Le titulaire ne garantit pas, par la seule fourniture de ces informations, la conformité réglementaire du bénéficiaire.

7.7.5 Prestations personnalisées

Les analyses spécifiques portant sur l'environnement propre d'un bénéficiaire, notamment la cartographie détaillée des composants déployés, l'analyse d'exposition, l'audit, le plan de remédiation ou l'assistance à la mise en œuvre, peuvent être commandées au moyen des lignes de services professionnels du Lot 3.

La commande de ces prestations ne peut conditionner l'accès aux informations standards, bulletins de sécurité, alertes, avis de vulnérabilité, correctifs, contournements ou justificatifs exigés par le présent article.

7.8 Réversibilité avancée

[SEC-ADV-050] En complément de la réversibilité de base commune aux deux lots, le titulaire garantit une réversibilité avancée permettant au bénéficiaire de reprendre l'exploitation ou d'en transférer la gestion à un tiers tout en limitant la rupture de protection et de service. Elle couvre les éléments techniques, documentaires, administratifs, de sécurité et contractuels nécessaires à la poursuite de l'exploitation.

Modalités techniques attendues

- restitution des configurations, sauvegardes, inventaires, licences, schémas, matrices de flux, politiques de sécurité, règles, objets, certificats et procédures à jour
- export des données d'administration, de supervision, des journaux et des référentiels dans des formats documentés et exploitables, sous réserve des durées de conservation applicables
- restitution ou suppression contrôlée des accès, comptes, certificats, secrets, jetons, clés, moyens de télémaintenance et délégations
- assistance à la reprise, transfert de connaissances, accompagnement du tiers repreneur et participation aux opérations de bascule
- vérification du maintien des fonctions de sécurité essentielles pendant la transition et définition des mesures compensatoires
- identification préalable des limitations, coûts, délais, dépendances, conditions de sortie et éléments non exportables.

Livrables attendus

N°	Livrable principal attendu
1	plan de réversibilité maintenu à jour
2	dossier final de transfert, inventaire contradictoire et archive des configurations
3	matrice de restitution des accès, comptes, certificats, secrets et moyens de télémaintenance
4	procès-verbal de transfert, de suppression des accès et de clôture de la réversibilité

Référence de prix

Référence	Libellé	Unité de prix
P4805	Forfait de réversibilité avancée incluant les livrables contractuels, l'assistance à la reprise et les opérations de sécurisation de la transition.	Forfait par périmètre technique

PIÈCE DE RÉPONSE : le candidat décrit précisément son organisation, ses moyens, ses engagements, les limites éventuelles, les justificatifs associés et, lorsqu'une référence tarifaire est prévue, les éléments de prix correspondants dans le cadre de réponse technique et dans le BPU.

7.9 Cohérence avec les pièces du marché

Le candidat assure la cohérence entre le CRT, les références SEC-ADV, le BPU, le DQE, les engagements de service et les justificatifs. Toute réserve, exclusion, dépendance, hypothèse ou condition affectant une exigence ou un prix est explicitement indiquée dans le CRT.

Les fournitures et prestations communes restent décrites et tarifées selon les pièces du Lot 3. Elles ne sont ni dupliquées ni facturées une seconde fois. La seule référence de prix spécifique prévue par le présent CCTP est P4805, sous réserve de sa concordance finale avec le BPU, le DQE et le CRT. Le candidat peut proposer, le cas échéant, un engagement de GTR renforcée, notamment de deux heures H24/7, dans les conditions prévues au BPU et au CRT

En cas d'écart entre une documentation commerciale et un engagement exprès figurant dans l'offre ou les pièces contractuelles, l'engagement exprès le plus contraignant pour le titulaire s'applique, sous réserve de la hiérarchie des pièces fixée au CCAP.