**CAHIER DES CHARGES**

**DU MARCHE PUBLIC DE**

**SERVICES**

**AYANT POUR OBJET UN ACCORD CADRE POUR**

**“CENTRALE D'ACHAT POUR PRESTATIONS D’ACCOMPAGNEMENT EN MATIÈRE DE CYBERSÉCURITÉ”**

**PROCÉDURE OUVERTE**

**Pouvoir adjudicateur**

**IMIO**

**Auteur de projet**

**IMIO, Frédéric Rasic**

**Rue Léon Morel, 1 à 5032 Isnes**

**Table des matières**

[**I.**](#_heading=h.gjdgxs) **Dispositions administratives 5**

[I.1](#_heading=h.1fob9te) Description du marché 5

[I.2](#_heading=h.3znysh7) Contexte de ce marché 6

[I.3](#_heading=h.2et92p0) Identité de l’adjudicateur 7

[I.4](#_heading=h.tyjcwt) Procédure de passation 7

[I.5](#_heading=h.3dy6vkm) Fixation des prix 7

[I.6](#_heading=h.1t3h5sf) Motifs d’exclusion et sélection qualitative 7

[I.7](#_heading=h.4d34og8) Questions et informations préalables au dépôt des offres 11

[I.8](#_heading=h.2s8eyo1) Forme et contenu des offres 11

[I.9](#_heading=h.17dp8vu) Dépôt des offres 12

[I.10](#_heading=h.3rdcrjn) Ouverture des offres 13

[I.11](#_heading=h.26in1rg) Délai de validité 13

[I.12](#_heading=h.lnxbz9) Critères d’attribution de l’accord-cadre 13

[I.13](#_heading=h.1rvwp1q) Options et Variantes 14

[I.13.1](#_heading=h.4bvk7pj) Variantes 14

[I.13.2](#_heading=h.35nkun2) Options 14

[I.14](#_heading=h.1ksv4uv) Choix de l’offre 14

[I.15](#_heading=h.44sinio) Limites de la centrale d’achat 14

[I.16](#_heading=h.z337ya) Accord-cadre 15

[**II.**](#_heading=h.1y810tw) **Dispositions contractuelles 16**

[II.1](#_heading=h.4i7ojhp) Fonctionnaire dirigeant 16

[II.2](#_heading=h.2xcytpi) Sous-traitants 16

[II.3](#_heading=h.1ci93xb) Assurances 17

[II.4](#_heading=h.2bn6wsx) Cautionnement 18

[II.5](#_heading=h.qsh70q) CV Vitrines 18

[II.6](#_heading=h.3as4poj) Clause de réexamen : Révisions de experts proposés 18

[II.7](#_heading=h.1pxezwc) Clause de réexamen : Révisions de prix 18

[II.8](#_heading=h.49x2ik5) Durée et délai d’exécution 19

[II.9](#_heading=h.2p2csry) Sanctions 19

[II.10](#_heading=h.147n2zr) Procédure de commande 19

[II.11](#_heading=h.3o7alnk) Procédure de facturation et Délai de paiement 19

[II.12](#_heading=h.23ckvvd) Délai de garantie 20

[II.13](#_heading=h.ihv636) Réception 20

[II.14](#_heading=h.32hioqz) Ressortissants d’un pays tiers en séjour illégal 20

[II.15](#_heading=h.1hmsyys) Rémunération due à ses travailleurs 20

[II.16](#_heading=h.41mghml) Protection des données 21

[II.17](#_heading=h.2grqrue) Devoir de réserve et confidentialité 21

[II.18](#_heading=h.3fwokq0) Pénalités 21

[II.19](#_heading=h.1v1yuxt) Compétence juridictionnelle et législation applicable 21

[II.20](#_heading=h.2u6wntf) Règlement Général de Protection des Données 22

[II.21](#_heading=h.19c6y18) Centrale d’achat & Accord cadre 24

[II.21.1](#_heading=h.3tbugp1) Limites de la centrale d’achat 25

[II.21.2](#_heading=h.28h4qwu) Conditions d’accès 25

[II.21.3](#_heading=h.nmf14n) Principe de la cascade - Ordre de consultation des attributaires 25

[II.21.4](#_heading=h.37m2jsg) Procédure de commande 26

[II.21.5](#_heading=h.48pi1tg) Procédure de réception des livraisons, implémentations et prestations 26

[II.21.6](#_heading=h.1mrcu09) Moyens de contrôles 26

[II.21.7](#_heading=h.1302m92) Fonctionnaire dirigeant 26

[II.21.8](#_heading=h.3mzq4wv) Accord de non-divulgation 27

[**III.**](#_heading=h.2250f4o) **Description des exigences techniques 28**

[III.1](#_heading=h.haapch) Introduction 28

[III.1.1](#_heading=h.319y80a) Objectif 28

[III.1.2](#_heading=h.1gf8i83) Contexte 28

[III.1.3](#_heading=h.40ew0vw) Domaines d’expertises 29

[III.1.4](#_heading=h.2fk6b3p) Glossaire 29

[III.2](#_heading=h.upglbi) Exigences générales 31

[III.3](#_heading=h.3ep43zb) Descriptions des lots 33

[III.3.1](#_heading=h.1tuee74) LOT A1 - Rédaction et accompagnement des politiques de sécurité 33

[III.3.1.1](#_heading=h.4du1wux) Objectifs du lot 34

[III.3.1.2](#_heading=h.2szc72q) Caractéristiques spécifiques du lot 34

[III.3.1.3](#_heading=h.184mhaj) Spécificités techniques 35

[III.3.1.4](#_heading=h.3s49zyc) Domaines d’expertises 36

[III.3.1.5](#_heading=h.279ka65) Rapports et documentations 36

[III.3.1.6](#_heading=h.meukdy) Obligation de résultat 37

[III.3.2](#_heading=h.36ei31r) Lot A2 - Évaluation des vulnérabilités et « pen tests » 37

[III.3.2.1](#_heading=h.1ljsd9k) Objectifs du lot 37

[III.3.2.2](#_heading=h.45jfvxd) Caractéristiques spécifiques du lot 38

[III.3.2.3](#_heading=h.2koq656) Spécificités techniques 38

[III.3.2.4](#_heading=h.zu0gcz) Domaines d’expertise 38

[III.3.2.5](#_heading=h.3jtnz0s) Rapports et documentations 39

[III.3.2.6](#_heading=h.1yyy98l) Obligation de résultat 39

[III.3.3](#_heading=h.4iylrwe) Lot A3 - Campagne de test de phishing/vishing/social engineering 39

[III.3.3.1](#_heading=h.2y3w247) Objectifs du lot 39

[III.3.3.2](#_heading=h.1d96cc0) Caractéristiques spécifiques du lot 40

[III.3.3.3](#_heading=h.3x8tuzt) Spécificités techniques 41

[III.3.3.4](#_heading=h.2ce457m) Domaines d’expertises 41

[III.3.3.5](#_heading=h.rjefff) Rapports et documentations 42

[III.3.3.6](#_heading=h.3bj1y38) Obligation de résultat 42

[III.3.4](#_heading=h.1qoc8b1) Lot A4 - Cyber Threat Intelligence 43

[III.3.4.1](#_heading=h.4anzqyu) Objectifs du lot 43

[III.3.4.2](#_heading=h.2pta16n) Caractéristiques spécifiques du lot 43

[III.3.4.3](#_heading=h.14ykbeg) Spécificités techniques 43

[III.3.4.4](#_heading=h.3oy7u29) Domaines d’expertise 44

[III.3.4.5](#_heading=h.243i4a2) Rapports et documentations 45

[III.3.4.6](#_heading=h.j8sehv) Obligation de résultat 45

[III.3.5](#_heading=h.338fx5o) Lot A5 - Accompagnement DPD/DPO à la demande 45

[III.3.5.1](#_heading=h.1idq7dh) Objectifs du lot 46

[III.3.5.2](#_heading=h.2olpkfy) Caractéristiques spécifiques du lot 46

[III.3.5.3](#_heading=h.13qzunr) Réglementations en vigueur 46

[III.3.5.4](#_heading=h.3nqndbk) Domaines d’expertise 47

[III.3.5.5](#_heading=h.22vxnjd) Rapports et documentations 47

[III.3.5.6](#_heading=h.i17xr6) Obligation de résultat 47

[III.3.6](#_heading=h.320vgez) Lot A6 - RSSI as a service 48

[III.3.6.1](#_heading=h.1h65qms) Objectifs du lot 48

[III.3.6.2](#_heading=h.415t9al) Caractéristiques spécifiques du lot 49

[III.3.6.3](#_heading=h.2gb3jie) Réglementations en vigueur 49

[III.3.6.4](#_heading=h.vgdtq7) Domaines d’expertises 49

[III.3.6.5](#_heading=h.3fg1ce0) Rapports et documentations 50

[III.3.6.6](#_heading=h.1ulbmlt) Obligation de résultat 50

**Auteur de projet**

Nom : IMIO

Adresse : Rue Léon Morel, 1 à 5032 Isnes

Personne de contact : M. Frédéric Rasic

Téléphone : 081/586.100

Fax : 081/586.129

E-mail : marche.public@imio.be

**Réglementation en vigueur**

1. Loi du 17 juin 2016 relative aux marchés publics et ses modifications ultérieures.

2. Arrêté royal du 18 avril 2017 relatif à la passation des marchés publics dans les secteurs classiques, et ses modifications ultérieures.

3. Arrêté royal du 14 janvier 2013 établissant les règles générales d'exécution des marchés publics, et ses modifications ultérieures.

4. Loi du 17 juin 2013 relative à la motivation, à l’information et aux voies de recours en matière de marchés publics, de certains marchés de travaux, de fournitures et de services et de concessions, et ses modifications ultérieures.

5. Règlement général pour la protection du travail (RGPT), Loi sur le bien-être et Code du bien-être au travail.

6. Loi du 11 février 2013 prévoyant des sanctions et des mesures à l’encontre des employeurs de ressortissants de pays tiers en séjour illégal.

7. Le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, et la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

**Dérogations, précisions et commentaires**

L’article 7 de l’arrêté royal du 14 janvier 2013 établissant les règles générales d’exécution des marchés publics dispose que *« Le présent chapitre et les articles 12, § 4, 37 à 38/19 et 61 à 63 sont applicables à l'accord-cadre. En ce qui concerne les marchés conclus sur la base de l’accord-cadre, l’ensemble des dispositions, sans préjudice des articles 5 et 6, sont d’application, sauf disposition contraire dans les documents du marché. Pour les marchés visés, il ne peut cependant être dérogé aux dispositions des articles 9, §§ 2 et 3, 12/1, 37 à 38/6, 38/8, 38/9, § 4, 38/10, § 4, 38/11 à 38/19, 62, alinéa 1er, 1°, et alinéa 2, 62/1 et 69* ».

En d’autres termes, l’arrêté royal du 14 janvier 2013 précité s’applique à l’accord-cadre et aux marchés fondés sur l’accord-cadre, sauf disposition contraire dans le cadre du présent cahier et sauf les dispositions expressément précitées.

En l’espèce, il est précisé que l’article 25 de l’arrêté royal du 14 janvier 2013 ne trouvera pas à s’appliquer : Il est dérogé à l'article 25 § 1er, 2°, h) de l'arrêté royal du 14 janvier 2013 établissant les règles générales d'exécution des marchés publics afin d'éviter les lourdeurs administratives rendues inutiles par le montant de certaines commandes, le cautionnement de 5% n'est exigé que pour les commandes subséquentes à ce marché et supérieures au montant de 50.000 €.

**Modifications apportées à ce document dans le cadre de l’erratum**

Pages 35/36 – Suppression de mentions SOC

Pages 38/39 – Description du forfait attendu dans le bordereau de prix

Pages 60-61-32 – Annexe B – ajout ligne lié au logiciel/service nécessaire

Page 90 – Annexe D – correction marque d’intérêt (Onhaye 🡺 Olne) + Ajout Hamois

# Dispositions administratives

Cette première partie se rapporte à la réglementation relative à la passation d'un marché public jusqu'à la désignation des adjudicataires.

Les dispositions contenues dans cette partie se rapportent à la loi du 17 juin 2016 et à l’arrêté royal du 18 avril 2017 et leurs modifications ultérieures.

## Description du marché

iMio a pour objectif de promouvoir et de coordonner la mutualisation de solutions métiers, de produits et services pour les pouvoirs locaux.

iMio est articulée autour de trois activités principales :

* Produire des logiciels Open source répondant aux besoins des pouvoirs locaux. Le modèle Open source permet à IMIO d'avoir la maîtrise des outils et d'avoir le choix du prestataire pour la réalisation de développements. Une partie des développements est assurée en interne, ce qui garantit une plus grande autonomie d'action ;
* Acheter des solutions en centrale d'achats pour permettre aux communes de bénéficier de solutions du marché à moindre coût et offrir un service d'accompagnement à leur utilisation et leur évolution ;
* Accompagner les membres et formaliser les projets informatiques des pouvoirs locaux (organisationnel).

La philosophie est celle de la mutualisation dans la logique « bottom-up » et efforts partagés pour réduire les coûts pour les membres, tout en produisant des solutions en permanence mieux adaptées aux réalités des pouvoirs locaux, puisque ce sont eux qui les produisent ou les font produire. Il est fondamental que les soumissionnaires adhèrent à ce mode de fonctionnement afin de garantir une adoption massive du projet grâce à l’adéquation fonctionnelle existant entre la réalité des Pouvoirs locaux et leurs outils informatiques.

Les candidats soumissionnaires doivent prendre ceci pour acquis et soumissionner dans cet état d’esprit et vision future.

**Objet du présent marché :** Établir une centrale d’achats en matière de cybersécurité

L’objectif de ce projet, passé sous la forme d’un accord cadre en vue d’établir une centrale d’achat pour ce marché, au profit des pouvoirs locaux wallon est de leur mettre à disposition un catalogue d’équipement (matériels et logiciels) et de services leur permettant de préserver la continuité de service de leurs missions et la protection des données de leurs citoyens.

Ce marché se compose de lots distincts couvrant un éventail de services liés à la cybersécurité, comprenant :

* Lot A1 : Rédaction et accompagnement à la mise en œuvre des politiques de sécurité
* Lot A2 : Évaluation des vulnérabilités et « Pen-tests »
* Lot A3 : Campagne de test de phishing/vishing/social engineering
* Lot A4 : Cyber threat intelligence
* Lot A5 : Accompagnement dpd/dpo à la demande
* Lot A6 : RSSI as a service

Le paysage des menaces en matière de cybersécurité étant en constante évolution, les Pouvoirs locaux se doivent d'être en mesure de faire face à ces défis pour garantir leur résilience et protéger leurs intérêts et ceux de leurs citoyens. Cette procédure ouverte est le résultat de la grande campagne d'audit menée ces derniers mois avec pour objectif de mettre en place un socle commun de défense pour la Wallonie. L'objectif de ce marché est de fournir aux communes et CPAS de Wallonie une solution de cybersécurité complète et personnalisée qui répondra à leurs besoins spécifiques en matière de protection contre les cybermenaces.

**Lieu de livraison** : Pouvoirs locaux wallons ayant adhéré à la centrale d’achat. La liste est reprise en annexe D au présent cahier spécial des charges.

**Codes CPV :**

* 73431000-2 Test et Évaluation de matériel de sécurité
* 79417000-0 Services de conseil en matière de sécurité.
* 79700000-1 Services d'enquête et de sécurité.

## Contexte de ce marché

Ce marché fait suite à l’établissement d’un état des lieux des Pouvoirs locaux concernant leur infrastructure, les mesures prises pour lutter contre la cybercriminalité et leur gouvernance réalisé entre septembre 2022 et mars 2023. L’objectif de ce marché est de répondre aux constats de l’exercice précédent par une offre pertinente d’équipements et logiciels aux Pouvoirs locaux afin de leur permettre de préserver la continuité de service de leurs missions et la protection des données de leurs citoyens. Ce marché vise à répondre aux constats issus de l'état des lieux que nous avons réalisé concernant l'infrastructure, les mesures de lutte contre la cybercriminalité et la gouvernance des Pouvoirs locaux en matière de sécurité de l’information.

Le gouvernement wallon a confié à iMio le rôle de pouvoir adjudicateur pour plusieurs projets visant à soutenir les Pouvoirs locaux dans leur lutte contre la cybercriminalité et la protection de leur cybersécurité. Ce projet de mutualisation et de valorisation des ressources liées à la cybersécurité vise à créer une base commune de cyberdéfense en Wallonie, afin de renforcer la protection de tous les Pouvoirs locaux face aux menaces en ligne en matière de cybercriminalité.

La mise en place d'une structure centralisée disposant de moyens d'action est devenue indispensable pour assurer la sécurité de l'ensemble des Pouvoirs locaux face à la croissance constante des risques en ligne. Ce projet de mutualisation et de valorisation des actifs liés à la cybersécurité a pour vocation de mener à l’émergence d’un « socle commun » de cyberdéfense en Wallonie. Avoir une structure centralisatrice disposant de moyens d’action est désormais indispensable tant la menace pèse sur l’ensemble des pouvoirs locaux.

Cette stratégie a été construite en collaboration totale avec les administrations compétentes sur les sujets de cybersécurité et s’énonce comme ceci

1. Mettre en place des solutions de cybersécurité à destination des communes de Wallonie, quelle que soit leur taille ;
2. Développer la connaissance des agents des pouvoirs locaux wallons à la réalité des menaces en matière de cybercriminalité et les sensibiliser aux bonnes pratiques en la matière pour qu’ils puissent s’en protéger ;
3. Soutenir l’action du Gouvernement wallon dans la transition numérique des pouvoirs locaux;
4. Créer un cadre numériquement sain pour aider les collectivités à travailler dans un environnement où disponibilité, intégrité et confidentialité seront les maîtres-mots;
5. Créer une centrale d’achats dédiée à la cybersécurité pour optimiser les investissements publics par le regroupement des communes de Wallonie et d’autres administrations.

La démarche de cyber-résilience est une approche globale qui se décompose en cinq étapes énoncées ci-dessous, le point de départ étant l’identification de la maturité de chaque pouvoir local de Wallonie face aux cyberattaques. Il convient de réaliser un état des lieux précis de ce qui est mis en place pour se protéger des cybermenaces. Ainsi, en comparant avec ce qu’il faudrait mettre en place, une série d’indicateurs, une analyse de la situation et un plan d’action seront définis.

Ce premier élément du socle commun fournira un résultat complet des audits de sécurité de chaque pouvoir local ayant fait appel à cette centrale d’achat. Les résultats de cette première étape ont pour objectif de déterminer les outils et mesures à intégrer dans la future centrale d’achat de fournitures et services , en fonction des catégories des pouvoirs locaux. Ces outils regrouperont les cinq piliers de la cybersécurité :

* Anticiper
* Prévenir
* Protéger
* Détecter et répondre
* Restaurer

La démarche de cyber résilience a pour but de garantir la confidentialité, l’intégrité et la disponibilité de l’information au sein des Pouvoirs locaux wallons.

La démarche s’inscrira également dans une logique cyclique d’amélioration continue en adéquation avec les bonnes pratiques en la matière, de type : planifier (Plan), développer ou réaliser (Do), contrôler (Check) et agir ou ajuster (Act), Cfr Roue de Deming.

## Identité de l’adjudicateur

IMIO

Rue Léon Morel, 1

5032 Isnes

Le pouvoir adjudicateur agit comme **centrale d’achat** au sens de l’article 2, 6°, a) de la Loi du 17 juin 2016 relative aux marchés publics, via la technique de l’accord-cadre.

IMIO agit comme pouvoir adjudicateur qui établit la centrale d’achat des services visés par le présent accord-cadre, au bénéfice des pouvoirs adjudicataires bénéficiaires (PAB).

Les pouvoirs adjudicateurs bénéficiaires de la présente centrale sont listés en annexe D du présent cahier spécial des charges.

Le déroulement des procédures subséquentes à ce marché initial est explicité dans la section « Accord cadre » du présent cahier spécial des charges.

## Procédure de passation

Le marché est passé par procédure ouverte.

## Fixation des prix

Le présent marché consiste en un marché à bordereau de prix.

Le marché à bordereau de prix est celui dans lequel les prix unitaires des différents postes sont forfaitaires et les quantités, pour autant que des quantités soient déterminées pour les postes, sont présumées ou exprimées dans une fourchette. Les postes sont portés en compte sur la base des quantités effectivement commandées et mises en œuvre.

Le marché est attribué sur base des prix unitaires mentionnés dans l'offre. Au moment de la rédaction des conditions du présent marché, le pouvoir adjudicateur n'est pas en mesure de définir avec précision les quantités de services dont il aura besoin. En conséquence, les quantités présumées indiquées au cahier des charges régissant le présent marché sont à titre purement indicatif, elles n'engagent nullement l'administration. Dès lors, les adjudicataires ne pourront réclamer aucune indemnité dans le cas où les quantités présumées ne seraient pas atteintes.

## Motifs d’exclusion et sélection qualitative

L'opérateur économique produit le Document unique de marché européen, qui consiste en une déclaration sur l'honneur propre actualisée et qui est accepté par le pouvoir adjudicateur à titre de preuve a priori en lieu et place des documents ou certificats délivrés par des autorités publiques ou des tiers pour confirmer que l'opérateur économique concerné :

1° ne se trouve pas dans l'une des situations d'exclusion visées aux articles 67 à 69 de la loi du 17 juin 2016;

2° répond aux critères de sélection applicables qui ont été établis conformément à l'article 71 de la loi du 17 juin 2016;

Marche à suivre pour compléter le DUME :

- Rendez-vous sur le site https://dume.publicprocurement.be, et choisissez votre langue.

- A la question ‘Qui êtes-vous’, répondez ‘Je suis un opérateur économique’.

- A la question ‘Quelle action souhaitez-vous effectuer ?’, répondez ‘Générer réponse’.

- Complétez votre pays et cliquez sur suivant.

- Parcourez le formulaire et répondez aux questions des parties ‘Procédure’ et ‘Exclusions’.

- Pour la partie ‘Sélection’, à la question ‘Souhaitez-vous utiliser les critères de sélection A à D ?’ répondez non. Dans ce cas, il vous est demandé une indication globale pour les critères de sélection.

- Précisez si vous satisfaites à tous les critères de sélection exigés.

- Après avoir complété l’entièreté du formulaire, cliquez sur ‘Aperçu’ en bas de page. Vous arrivez sur votre DUME complété que vous pouvez télécharger au format PDF et/ou xml pour être fourni électroniquement avec votre offre.

Les opérateurs économiques peuvent réutiliser un DUME qui a déjà été utilisé dans une procédure antérieure, à condition qu'ils confirment que les informations qui y figurent sont toujours valables.

**L’attention des soumissionnaires est attirée sur le fait qu'un DUME doit être déposé pour tout sous-traitant, quel que soit son statut (indépendant, freelance, ...) à la compétence duquel il est fait appel en vue de satisfaire aux conditions posées au titre de la sélection qualitative.**

Le pouvoir adjudicateur vérifiera, via l'application Télémarc ou via d'autres applications électroniques équivalentes et accessibles gratuitement dans d'autres États membres, la situation du soumissionnaire sur le plan des dettes sociales et sa situation fiscale dans les 20 jours suivant la date ultime pour l'introduction des offres.

L’extrait de casier judiciaire sera examiné dans le chef des attributaires pressentis, ainsi que dans le chef des membres de l'organe administratif, de gestion ou de surveillance desdits attributaires pressentis ou détiennent un pouvoir de représentation, de décision ou de contrôle en leur sein.

**Situation juridique du soumissionnaire (motifs d'exclusion)**

\* Le DUME, par lequel l'opérateur économique déclare qu’il ne se trouve pas dans une des situations d’exclusion visées aux articles 67 à 69 de la loi du 17 juin 2016.

**L’attention des soumissionnaires est attirée sur le fait qu'un DUME doit être déposé pour tout sous-traitant, quel que soit son statut (indépendant, freelance, ...) à la compétence duquel il est fait appel en vue de satisfaire aux conditions posées au titre de la sélection qualitative.**

**Les soumissionnaires fourniront d’initiative les éventuelles mesures correctrices tant aux clauses d’exclusion obligatoire qu’aux clauses d’exclusion facultative.**

**Capacité technique et professionnelle du soumissionnaire (critères de sélection)**

Le DUME de l'opérateur économique et/ou éventuellement d’un ou plusieurs sous-traitants auquel il est fait appel, par le/lesquels le soumissionnaire déclare qu'il satisfait aux critères de sélection suivants :

| N° | Critères de sélection | Exigences minimales pour chaque expert |
| --- | --- | --- |
| 1 | Proposer au minimum 1 experts[[1]](#footnote-0) cybersécurité Senior pour l’exécution des missions, les experts doivent satisfaire aux exigences minimales. | * Expérience professionnelle approfondie :   + Minimum 7 ans d'expérience professionnelle dans les domaines des lots concernés (ISO27001, NIS2, RGPD).   + Solide expérience et expertise dans le domaine de la cybersécurité, démontrant la capacité à gérer des défis complexes liés à la sécurité de l'information   + Certification pertinente en cybersécurité. * Connaissance technique avancée :   + Au moins 5 ans d'expérience professionnelle dans les aspects techniques de la cybersécurité, la conception d'architecture TIC, la protection des données et la mise en œuvre des TIC (ISO27001, NIS2).   + Capacité à résoudre des problèmes techniques complexes et à proposer des solutions innovantes pour renforcer la sécurité des systèmes d'information. * Expérience de projet pertinente dans les 3 dernières années, d’une mission de 30 jours-homme, à savoir :   + Expérience avérée dans des projets de recherche et développement, de services de conseil et de consultation conformes aux spécifications du lot soumissionné (ISO27001, RGPD).   + Références clients attestant de l'expertise et de la réussite dans la réalisation de projets similaires. * Connaissance des directives et lois en matière de cybersécurité :   + Connaissance approfondie des directives de l'UE, des lois nationales et des directives de l'UE concernant la cybersécurité (NIS2, RGPD).   + Familiarité avec les réglementations en vigueur et capacité à les appliquer dans les projets de cybersécurité. * Compétences en gouvernance de la sécurité :   + Expérience avérée par la validation d'un ou plusieurs clients en matière de gouvernance de la sécurité (ISO27001, RGPD).   + Capacité à fournir des conseils stratégiques, à élaborer des politiques de sécurité efficaces et à accompagner les clients dans leur mise en œuvre. * Maîtrise du français (écrit/parlé) |
| 2 | Proposer au minimum 1 experts1 cybersécurité junior pour l’exécution des missions, les experts doivent satisfaire aux exigences minimales. | * Formation et diplômes :   + Diplôme universitaire ou équivalent dans le domaine de la cybersécurité, des technologies de l'information ou des domaines connexes.   + Certification pertinente en cybersécurité. * Expérience professionnelle :   + Au moins 1 à 3 ans d'expérience professionnelle dans le domaine de la cybersécurité ou des technologies de l'information (ISO27001, NIS2).   + Expérience pratique dans la mise en œuvre des mesures de sécurité et la résolution des problèmes courants liés à la cybersécurité. * Connaissances techniques :   + Bonne compréhension des principes de base de la cybersécurité, y compris les concepts de confidentialité, d'intégrité et de disponibilité des données (ISO27001, NIS2).   + Connaissance des principaux outils et technologies de cybersécurité (pare-feu, antivirus, IDS/IPS, etc.). * Compétences analytiques :   + Capacité à analyser les vulnérabilités et les menaces potentielles, et à proposer des solutions appropriées (ISO27001, NIS2).   + Aptitude à effectuer des évaluations de sécurité de base et à recommander des mesures correctives. * Esprit d'équipe et communication :   + Capacité à travailler efficacement en équipe, à collaborer avec d'autres experts et à partager des informations pertinentes (ISO27001, NIS2).   + Bonnes compétences en communication verbale et écrite, permettant de présenter des rapports et de communiquer efficacement avec les clients. * Maîtrise du français (écrit/parlé) |
| 3 | Minimum 1 coordinateur de projet | Pour être sélectionné, l’équipe proposée doit disposer d’un coordinateur de projet répondant aux conditions cumulatives suivantes :   * Disposer d’une expérience en matière de coordination de projet de minimum 3 ans, expérience à attester par le curriculum vitae ; * Être inscrit sur le payroll du soumissionnaire pour des raisons de continuité et d’homogénéité de l’exécution des marchés subséquents sur la durée de l’accord cadre. |

Pour simplifier le travail de complétion du bordereau de sélection qualitative, iMio a préparé le présent document, librement téléchargeable et utilisable par les candidats soumissionnaires : <https://docs.google.com/spreadsheets/d/13WQI9ZAowh8lxotHEOW7GQliLt5Vnc0oebz1273T1m0/edit?usp=sharing>

## Questions et informations préalables au dépôt des offres

**Questions**

Jusqu’au 5/7/2023 à 10h00, les candidats-soumissionnaires peuvent adresser leurs questions relatives à cette procédure de marché à iMio :

* Adresse : IMIO, Rue Léon Morel 1, 5032 Isnes
* E-mail : [marche.public@iMio.be](mailto:marche.public@imio.be)

Au-delà de cette échéance, les questions ne seront plus recevables.

Les questions doivent être identifiées par :

* Un numéro de question
* Le nom du candidat-soumissionnaire
* La section du cahier spécial des charges faisant l’objet du questionnement
* Le numéro de page faisant l’objet du questionnement

Aucune question ne pouvant être contextualisée au cahier spécial des charges ne sera traitée.

Afin de simplifier le travail de questionnement et réponse, nous vous invitons à utiliser le document (libre de téléchargement) suivant pour poser vos questions sur le marché public : <https://docs.google.com/document/d/1DRnxBa0rnGjxXRhKzF_ysgDyJZEj3PHhoOuFUtPhh68/edit?usp=sharing>

**Séance d’information**

Sur base des questions posées et des réponses préparées par le pouvoir adjudicateur, une séance d’information sera organisée le 12/7/2023 à 13h30 par le biais d’une visioconférence. Cette information aura pour but de récapituler les éléments principaux du présent marché public ainsi que parcourir les questions-réponses posées par les soumissionnaires.

Pour participer à la séance d’information, le soumissionnaire doit s’inscrire préalablement par mail :

* Adresse mail : [marche.public@imio.be](mailto:marche.public@imio.be)
* Contenu du mail :
  + Sujet : Marché Cybersécurité iMio – « Nom du soumissionnaire »
  + Contenu du mail : coordonnées des participants (nom, prénom, numéro de portable et adresse mail)

Seuls les soumissionnaires peuvent participer à la séance d’information, le pouvoir adjudicateur rappelle que cette séance d’information se fait sur base volontaire, il ne s’agit pas d’une obligation légale, qu’il est donc attendu des participants une attitude correcte et une participation active dans le cadre autorisé par la procédure ouverte. Ne s’agissant pas d’une procédure négociée, aucun terme du cahier spécial des charges ne peut être adapté/modifié.

Les soumissionnaires peuvent poser des questions complémentaires durant la séance d’information, le pouvoir adjudicateur se réserve le droit de ne pas répondre directement en séance et de fournir la réponse par le biais de la publication via Public Procurement (Cfr ci-dessous).

Les questions relevantes, leurs réponses et les documents de la séance d’information seront mis à disposition par l’intermédiaire de Public Procurement au plus tard le 19/7/2023.

## Forme et contenu des offres

Le soumissionnaire établit son offre en français et complète l'inventaire sur le modèle annexé au cahier des charges le cas échéant. Les soumissionnaires ne sont pas autorisés à établir leur offre sur d'autres documents que le formulaire prévu quand bien même il supporte l'entière responsabilité de la parfaite concordance entre les documents qu'il a utilisés et le formulaire.

Les offres étant transmises par des moyens électroniques, le rapport de dépôt de l'offre doit être revêtu d'une signature électronique qualifiée.

Lorsque le rapport de dépôt est signé par un mandataire, celui-ci mentionne clairement son (ses) mandant(s). Le mandataire joint l'acte authentique ou sous seing privé qui lui accorde ses pouvoirs ou une copie scannée de la procuration.

**L’attention du soumissionnaire est attirée sur le fait que la signature du rapport de dépôt par une personne (physique ou morale) non compétente pour engager celui-ci entrainera l'irrégularité de l’offre.**

Les prix doivent toujours être exprimés en euro.

**Pour qu’une offre soit valable, elle doit contenir les éléments suivants présentés :**

Le DUME ainsi que pour les lots soumissionnés :

* Annexe A : formulaire d’offre
* Annexe B : Inventaire
  + Une première version faisant apparaître tous les articles, logiciels et prestations qui peuvent être nécessaires au cours de l’exécution du présent marché, et cela sur un bordereau différent pour chaque lot auquel le soumissionnaire souhaite participer ;
  + Une deuxième version du tableau précédent, où le modèle économique exposé est mis en application pour répondre au scénario, et cela sur un bordereau différent pour chaque lot auquel le soumissionnaire souhaite participer.
* Annexe C : Bordereau(x) de réponse technique
* Annexe G : Engagements sur l’obligation de résultats
* Un document récapitulatif de l’offre de service proposée ainsi qu’une présentation de la société ;
* Les curriculums vitae des personnes les identifiant de manière unique
* Les fiches produits/services nécessaires
* Toute(s) autre(s) annexe(s) nécessaire(s) à la bonne complétion du dossier

**Modification des quantités présumées**

Le pouvoir adjudicateur n’autorise pas les soumissionnaires à corriger dans les offres les erreurs relatives à l’estimation des quantités présumées.

**Sous-traitance**

Le soumissionnaire indique dans son offre la part du marché qu'il a l'intention de sous-traiter ainsi que les sous-traitants proposés, si connus.

**Soumission à plusieurs lots**

Si le soumissionnaire répond à plusieurs lots, il ne peut pas proposer de rabais, ni d’améliorations.

## Dépôt des offres

Seules les offres qui sont envoyées au plus tard avant l’ouverture des offres via le site internet e-Tendering https://eten.publicprocurement.be/ seront acceptées par le pouvoir adjudicateur. Le site internet e-Tendering garantit le respect des conditions établies par l'article 14, §7 de la loi du 17 juin 2016.

Il y a lieu de remarquer que l'envoi d'une offre par e-mail ne répond pas à ces conditions. Dès lors, il n'est pas autorisé d'introduire une offre par ce moyen.

Par le seul fait de présenter une offre totalement ou partiellement par des moyens électroniques, le soumissionnaire accepte que les données découlant du fonctionnement du dispositif de réception de son offre soient enregistrées.

Plus d'informations peuvent être obtenues sur le site : http://www.publicprocurement.be ou via le numéro de téléphone du helpdesk du service e-Procurement : +32 (0)2 740 80 00.

**L'offre ne peut pas être introduite sur papier.**

Par l’introduction d’une offre, les soumissionnaires acceptent sans condition le contenu du cahier des charges et des autres documents relatifs au marché, ainsi que le respect de la procédure de passation telle que décrite dans le cahier des charges et acceptent d’être liés par ces dispositions.

Lorsqu’un soumissionnaire formule une objection à ce sujet ou lorsqu'il découvre des erreurs ou des omissions dans les documents du marché, telles qu’elles rendent impossible l’établissement de son prix ou la comparaison des offres, il les signale immédiatement par écrit et par courrier recommandé, et ce, au plus tard 10 jours avant la date et l'heure limites d'introduction des offres.

Le soumissionnaire est tenu de signaler tout problème de légalité immédiatement apparent à l’égard de la procédure ou du présent cahier spécial des charges, afin qu’il puisse, si nécessaire, encore y être rectifié en ayant le moins de répercussions possibles sur le déroulement de la procédure d’attribution. À défaut de l’avoir fait au plus tard dans les 10 jours de la date ultime de dépôt des offres, le soumissionnaire n’est plus fondé à s’en prévaloir ultérieurement.

## Ouverture des offres

Le : 21/8/2023 à 10h00.

Les offres sont introduites électroniquement, il n'y a pas d'ouverture des offres en séance publique.

## Délai de validité

Le soumissionnaire reste lié par son offre pendant un délai de 120 jours de calendrier, à compter de la date limite de réception des offres.

## Critères d’attribution de l’accord-cadre

Les critères suivants sont d'application lors de l'attribution de l’accord-cadre :

| **N°** | **Description** | **Pondération** |
| --- | --- | --- |
| 1 | Prix | 70 |
|  | *Score offre = (prix de l’offre la plus basse / prix de l’offre) \* pondération du critère « Prix »* | |
| 2 | Qualité des services | 30 |
|  | *2.1 Maîtrise des domaines d'expertise (15 Pts) - Les domaines d’expertise confirmés seront cotés à 1, le résultat de chaque expert sera obtenu par la sommes des côtes individuelles des domaines d’expertise, le niveau du soumissionnaire sera obtenu par la moyenne arithmétique des experts présentés par celui-ci. Les résultats seront comparés entre eux par une règle de 3.*  *Score offre = (résultat du soumissionnaire / résultat maximal) \* pondération du critère « Maîtrise des domaines d’expertise »*  *2.2 Qualité des méthodologies et documentations (15 pts) - Ces éléments seront évalués par des questions ouvertes (annexe C). Chaque réponse aux questions posées sera évaluée par une note allant de 1 à 10. Les résultats individuels seront sommés et comparés entre eux par une règle de 3.*  *Score offre = (résultat du soumissionnaire / résultat maximal) \* pondération du critère « Qualité des méthodologies et documentations »* | |
| Pondération totale des critères d'attribution : | | 100 |

Une certaine valeur a été attribuée à chaque critère. Sur base de l'évaluation de tous ces critères, tenant compte de la valeur attribuée à chacun, un classement des offres sera réalisé pour chacun des lots de l’accord cadre.

Ces critères d’attributions sont utilisés pour établir l’ordre de la cascade (Cfr parties relatives à accord-cadre). Les marchés subséquents ne sont pas remis en concurrence (application de la cascade).

## Options et Variantes

La distinction qui est faite entre option et variante se décrit comme suit :

* Une variante est un élément encadré par le pouvoir adjudicateur et proposé à l’initiative de l’attributaire, qui remplace en partie la demande du pouvoir adjudicateur ;
* Une option est un élément qui vient compléter un équipement/service, sans le remplacer.

## Variantes

Aucune variante (libre ou facultative) n’est prévue ou autorisée.

## Options

Aucune variante (libre ou facultative) n’est prévue ou autorisée.

## Choix de l’offre

Le pouvoir adjudicateur choisit l'offre économiquement la plus avantageuse, déterminée en se fondant sur le meilleur rapport qualité / prix.

Par la présentation de son offre, le soumissionnaire accepte toutes les clauses du Cahier des Charges et renonce à toutes les autres conditions. Si le pouvoir adjudicateur constate, lors de l’analyse des offres, que le soumissionnaire a ajouté des conditions qui rendent l’offre imprécise ou si le soumissionnaire émet des réserves quant aux conditions du Cahier des Charges, le pouvoir adjudicateur se réserve le droit de considérer l’offre comme substantiellement irrégulière.

Le pouvoir adjudicateur rectifie les erreurs dans les opérations arithmétiques et les erreurs purement matérielles dans les offres, sans que sa responsabilité soit engagée pour les erreurs qui n’auraient pas été décelées. Pour ce faire il peut, dans le délai qu’il détermine, inviter le soumissionnaire à préciser et à compléter la teneur de son offre sans la modifier, afin de rechercher l’intention réelle.

## Limites de la centrale d’achat

La présente centrale d’achat est limitée aux pouvoirs adjudicateurs bénéficiaires (PAB), à savoir, des pouvoirs locaux wallons ayant marqué un intérêt préalablement au lancement du présent marché et listés en annexe D du présent cahier spécial des charges.

Les marchés subséquents sont commandés par les PAB au fur et à mesure des besoins de ses membres. Ces données ne sont pas un engagement ferme de commande de la part du pouvoir adjudicateur et de ses membres. Ces données constituent une information à l’attention des soumissionnaires.

Le montant cumulé maximal qui pourra être attribué dans le cadre de marchés subséquents fondés sur cet accord cadre (tous lots confondus) est de 4.000.000 € TVAC. Une fois ce maximum atteint, aucun nouveau marché ne pourra plus être attribué via la centrale d’achat. La fin de la centrale d’achats ne porte pas préjudice à la poursuite de l’exécution des marchés subséquents en cours.

L’attention des soumissionnaires est attirée sur le fait que la conclusion de l’accord cadre n’entraîne aucune exclusivité dans leurs chefs, iMio se réservant donc le droit de satisfaire les besoins de ce présent marché par d’autres moyens (cfr absence d’exclusivité).

## Accord-cadre

**I.3.1. Principe**

Le marché est passé par accord-cadre pluri-attributaires.

Toutes les adjudicataires remettant une offre régulière et conforme seront reprises dans l’accord cadre et classée dans la cascade selon leur résultat obtenu via les critères d’attribution.

**I.3.2. Absence d’exclusivité**

La conclusion de l’accord-cadre n’implique :

* Aucun droit pour l’adjudicataire de fournir les biens et les services visés par le marché. Les quantités reprises dans l’inventaire sont des quantités présumées par le pouvoir adjudicateur aux fins de la remise et de la comparaison des offres. Elles ne constituent en rien des quantités minimales au sens des articles 148 et 151 RGE. Les marchés fondés sur l’accord-cadre seront attribués au fur et à mesure des besoins réels.
* Aucun droit d’exclusivité dans le chef de l’adjudicataire. L’adjudicataire ne peut de ce chef faire valoir aucun droit à un quelconque dédommagement ou à une quelconque révision du marché.

Le nombre de marchés subséquents n’est pas connu au stade de l’attribution de l’accord-cadre.

# Dispositions contractuelles

Cette deuxième partie fixe la procédure relative à l’exécution du marché.

Pour autant qu’il n’y soit pas dérogé, l'arrêté royal du 14 janvier 2013 et ses modifications ultérieures établissant les règles générales d'exécution des marchés publics est d’application.

## Fonctionnaire dirigeant

Le contrôle de la procédure initiale ainsi que d’éventuelles inspections des marchés subséquents se déroulent sous l’autorité du conseil d’administration d’iMio représenté par :

Nom : Mr Frédéric Rasic

Adresse : IMIO, Rue Léon Morel, 1 à 5032 Isnes

Téléphone : 081/586.100

Fax : 081/586.129

E-mail : marche.public@imio.be

Le conseil d’administration d’iMio est le seul compétent pour prendre des décisions dans le cadre de la procédure initiale. La personne désignée ci-avant est le représentant désigné par le fonctionnaire dirigeant permettant un contact entre le pouvoir adjudicateur et l’adjudicataire. Elle n’a pas autorité de décision.

L’exécution et la surveillance des fournitures et/ou services des marchés subséquents se déroulent sous le contrôle et la responsabilité du fonctionnaire dirigeant du pouvoir adjudicateur désigné par le membre bénéficiaire. Le fonctionnaire dirigeant peut se faire représenter par une personne physique. Dans ce cas, cette personne doit être désignée par le fonctionnaire dirigeant préalablement à l’attribution du marché subséquent.

Le fonctionnaire dirigeant est le seul compétent pour prendre des décisions en matière d’exécution. La personne désignée pour représentation permet un contact entre le pouvoir adjudicateur et l’adjudicataire. Elle n’a pas pouvoir de décision.

Mandats du fonctionnaire dirigeant et son représentant :

* Le fonctionnaire dirigeant est mandaté pour prendre toutes les décisions nécessaires, dans les limites imposées par le présent cahier spécial des charges, afin de veiller à la bonne exécution du contrat ;
* Toute promesse, modification ou accord qui diverge des conditions de ce Cahier spécial des Charges et qui n’est pas notifié par le pouvoir adjudicateur est à considérer comme nul par les deux parties ;
* Le fonctionnaire dirigeant peut déléguer tout ou partie de ses fonctions à un de ses délégués moyennant communication écrite aux participants concernés ;
* Le représentant du fonctionnaire dirigeant ne peut prescrire des services modificatifs ou supplémentaires quelconques sans l’accord écrit du Pouvoir adjudicateur.

Toutes communications et notifications que l’attributaire estime devoir faire concernant son marché sont faites, par écrit, au fonctionnaire dirigeant.

L’attributaire ne pourra se prévaloir du fait qu’une surveillance ou un contrôle a été exercé par le pouvoir adjudicateur ou son fonctionnaire dirigeant pour prétendre être dégagé de sa responsabilité si les travaux venaient à être refusés ultérieurement.

## Sous-traitants

Le soumissionnaire peut faire valoir les capacités de sous-traitants ou d'autres entités. Dans ce cas, il joint à son offre les documents utiles desquels ressort l'engagement de ces sous-traitants ou entités de mettre les moyens nécessaires à la disposition du soumissionnaire. **Le sous-traitant déposera son DUME.**

Si un opérateur économique souhaite recourir aux capacités d'autres entités pour sa sélection qualitative en ce qui concerne les critères relatifs aux titres d'études et professionnels ou à l'expérience professionnelle pertinente, l’opérateur économique est tenu de travailler avec ces sous-traitants désignés lors de l'exécution du marché. Le recours à d'autres sous-traitants est soumis à l'accord préalable du pouvoir adjudicateur.

En application de l'article 74 de l'AR du 18 avril 2017, le soumissionnaire indique dans son offre la part du marché qu'il a éventuellement l'intention de sous-traiter ainsi que les sous-traitants proposés.

Le pouvoir adjudicateur transmet, au plus tard au début de l’exécution du marché, les informations suivantes à l’adjudicateur : le nom, les coordonnées et les représentants légaux de tous les sous-traitants, quelle que soit la mesure dans laquelle ils participent à la chaîne de sous-traitance et quelle que soit leur place dans cette chaîne, participant à l'exécution du marché, dans la mesure où ces informations sont connues à ce stade.

Le pouvoir adjudicateur est, pendant toute la durée du marché, tenu de porter sans délai à la connaissance de l’adjudicateur de tout changement relatif à ces informations ainsi que des informations requises pour tout nouveau sous-traitant qui participera ultérieurement à ces travaux ou à la prestation de ces services.

Les adjudicataires demeurent responsables envers le pouvoir adjudicateur lorsqu'ils confient tout ou partie de leurs engagements à des sous-traitants.

Le pouvoir adjudicateur ne lie aucun lien contractuel avec ces sous-traitants.

Ces sous-traitants ne peuvent se trouver dans un des cas d'exclusion visés à l'article 67 de la loi du 17 juin 2016, hormis le cas où l'entrepreneur, le fournisseur ou le prestataire de services concerné, conformément à l'article 70 de la loi, démontre vis-à-vis de du pouvoir adjudicateur avoir pris les mesures suffisantes afin de prouver sa fiabilité.

En application de l'article 12/4 de l'AR du 14 janvier 2013, ces sous-traitants satisfont, proportionnellement à la partie du marché qu'ils exécutent, aux exigences minimales en matière de capacité technique et professionnelle imposées par les documents du marché.

**Sous-traitants**  
Dans le cadre de ce marché, la sous-traitance est autorisée au maximum d’un seul niveau :

* Attributaire du marché
  + Sous-traitant de niveau 1 : acceptable
    - Sous-traitant de niveau 2 : Interdit

Le candidat soumissionnaire doit joindre à son offre une déclaration de sous-traitance signée par le sous-traitant déclaré. À défaut de déclaration signée, l’offre du candidat soumissionnaire sera déclarée irrégulière.

## Assurances

Les adjudicataires contractent les assurances couvrant leur responsabilité en matière d'accidents de travail et leur responsabilité civile vis-à-vis des tiers lors de l'exécution du marché.

Dans un délai de trente jours à compter de la conclusion de l’accord cadre , l'adjudicataire justifie qu'il a souscrit ces contrats d'assurances, au moyen d'une attestation établissant l'étendue de la responsabilité garantie requise par les documents de l’accord cadre.

A tout moment durant l'exécution du marché, l'adjudicataire produit cette attestation, dans un délai de quinze jours à compter de la réception de la demande du pouvoir adjudicateur.

## Cautionnement

Aucun cautionnement n'est demandé.

**Article 25 de l'arrêté royal du 14 janvier 2013**

Aucun cautionnement n'est exigé alors qu'il est légalement obligatoire.

Justification : Il est dérogé à l'article 25 § 1er, 2°, h) de l'arrêté royal du 14 janvier 2013 établissant les règles générales d'exécution des marchés publics afin d'éviter les lourdeurs administratives rendues inutiles par le montant de certaines commandes, le cautionnement de 5% n'est exigé que pour les commandes, passées par les PAB et subséquentes à ce marché, supérieures au montant de 50.000 €. Les cautionnements seront donc constitués dans le cadre des marchés subséquents effectués par les pouvoirs adjudicateurs bénéficiaires de la centrale d’achat.

## CV Vitrines

Le soumissionnaire est tenu de faire participer aux missions les personnes qui ont été proposées en réponse à cet accord cadre. Le pouvoir adjudicateur entend ainsi interdire la pratique des CV-Vitrines. Les sanctions sont définies dans les dispositions contractuelles relatives à l’exécution (II.9 Sanctions).

## Clause de réexamen : Révisions de experts proposés

La pratique des CV Vitrine étant interdite, et vu les évolutions professionnelles possibles au cours de la durée de vie de la centrale d’achat, le remplacement des experts chargés des mission est autorisé, à condition qu’il :

* Présente les caractéristiques équivalentes au profil remplacé ;
* Ait été Sollicité au fonctionnaire dirigeant du pouvoir adjudicateur de cet accord-cadre ;
* Autorisé par ce dernier.

Seul iMio est compétent pour autorisé ce remplacement.

## Clause de réexamen : Révisions de prix

Une révision des prix sera autorisée, à fréquence annuelle. Elle est autorisée à la hausse et à la baisse mais sera plafonnée à une augmentation maximum équivalente à l’indexation annuelle de l’ipc lissé publié sur statbel.fgov.be.

Le soumissionnaire n’est pas autorisé à cumuler les augmentations non-réclamées pour justifier une révision dépassant le taux fixé.

La révision des prix demandée par le soumissionnaire doit être basée sur des paramètres objectifs et contrôlables, elle doit utiliser des coefficients de pondération appropriés, elle reflète ainsi la structure réelle des coûts.

Les motifs pouvant être invoqués sont, dans le cadre de l’activité de consultance :

* Licences :
  + Prix d’achat
  + Taux de change
* Matériel :
  + Prix d’achat
  + Taux de change
* Fournitures/énergies :
  + Prix d’achat
  + Taux de change
* Prestations :
  + Indice salaire

Les demande de révision des prix doivent être introduites par courrier, à l’attention du fonctionnaire dirigeant, au plus tard 2 mois avant la date échéance. La date échéance est l’anniversaire de l’attribution du marché (en pratique, si l’attribution du marché est décidée par le fonctionnaire dirigeant d’iMio le 1 juillet 2023, les demandes de révision des prix pour l’année suivante doivent être introduites au plus tard le 1 mai des années suivantes). À défaut de respecter le délai d’introduction, la demande de révision des prix sera ignorée, il sera interdit aux attributaires concernés d’adapter leur prix.

## Durée et délai d’exécution

Durée totale de cet accord-cadre : 48 mois

L’accord-cadre prend cours le premier jour calendrier qui suit le jour où les adjudicataires ont reçu la notification de la conclusion de l’accord-cadre.

Lorsque l’accord-cadre est résilié en application d’une mesure d’office ou en application de l’article II.9 du présent cahier, la résiliation de l’accord-cadre est limitée au seul attributaire à l’encontre de qui la mesure a été prise.

Délai d’exécution des marchés subséquents est à convenir lors de la commande

Le marché subséquent prend cours le premier jour calendrier qui suit le jour où iMio a reçu l’accusé de réception du bon de commande. Les marchés subséquents conclus avant la date d’échéance de l’accord-cadre demeurent exécutables jusqu’à leur terme.

## Sanctions

* + 1. **Attributaire**

Lorsqu’un adjudicataire est 2 fois d’affilée dans l’incapacité d’exécuter la mission, son classement dans la cascade des attributaires en est affecté, il perd une place au profit de l’attributaire qu’il précédait (rétrogradation).

Après 2 déclassements, cet attributaire peut être exclu de l’accord-cadre de la centrale d’achat par décision du fonctionnaire dirigeant.

* + 1. **Expert**

Lorsqu’un expert délivre à 2 reprises un travail incomplet ou incorrect (cfr. Vérification des factures envoyées, description des exigences techniques et annexes du présent cahier des charges), l’adjudicataire perd une place au profit de l’attributaire qu’il précédait (rétrogradation) et ce pour la durée de l’accord-cadre.

## Procédure de commande

Les informations relatives à la méthodologie de commande(s) subséquente(s) sont présentées dans la section « Centrale d’achat ».

## Procédure de facturation et Délai de paiement

Les modalités de facturation sont à définir par les pouvoirs adjudicateurs bénéficiaires, dans le cadre de leur(s) marché(s) subséquent(s).

**Facturation électronique**

Le pouvoir adjudicateur accepte la transmission des factures sous un format électronique (au format XML selon le standard PEPPOL bis), conformément à l'article 192/1 de la loi du 17/06/2016.

Les factures pourront être soumises directement via https://digital.belgium.be/e-invoicing/ ou via votre outil comptable (connecté au réseau PEPPOL).

La facture électronique doit obligatoirement comporter les mentions suivantes :

1° les identifiants de processus et de facture ;

2° la période de facturation ;

3° les renseignements concernant le vendeur ;

4° les renseignements concernant l’acheteur ;

5° les renseignements concernant le bénéficiaire du paiement ;

6° les renseignements concernant le représentant fiscal du vendeur ;

7° la référence du contrat ;

8° les détails concernant la fourniture ;

9° les instructions relatives au paiement ;

10° les renseignements concernant les déductions ou frais supplémentaires ;

11° les renseignements concernant les postes figurant sur la facture ;

12° les montants totaux de la facture ;

13° la répartition par taux de TVA.

En cas de retard de paiement, la somme s’impute d’abord sur le capital, puis sur les intérêts.

## Délai de garantie

Aucun délai de garantie n'est applicable pour ce marché.

## Réception

Les modalités de réception sont à définir par les pouvoirs adjudicateurs bénéficiaires, dans le cadre de leur(s) marché(s) subséquent(s), une procédure minimale est toutefois définie dans le cadre de la centrale d’achat (Cfr section Centrale d’achat).

## Ressortissants d’un pays tiers en séjour illégal

Lorsque l’adjudicataire ou sous-traitant reçoit copie de la notification visée à l’article 49/2, alinéa 4, du Code pénal social, dans laquelle il est informé qu’il occupe en Belgique un ou plusieurs ressortissants d’un pays tiers en séjour illégal, cet adjudicataire ou sous-traitant s’abstient, avec effet immédiat, de se rendre encore au lieu d’exécution du marché ou de poursuivre l’exécution du marché, et ce jusqu’à ce que l’autorité adjudicatrice donne un ordre contraire.

Il en va de même lorsque l’adjudicataire ou sous-traitant est informé :

- soit par l’adjudicataire ou par l’autorité adjudicatrice selon le cas de ce qu’ils ont reçu la notification, visée à l’article 49/2, alinéas 1er et 2, du Code pénal social, concernant cette entreprise ;

- soit via l’affichage prévu par l’article 35/12 de la loi du 12 avril 1965 relative à la protection de la rémunération des travailleurs, qu’il occupe en Belgique un ou plusieurs ressortissants d’un pays tiers en séjour illégal.

Par ailleurs, l’adjudicataire ou sous-traitant est tenu d’insérer, dans les contrats de sous-traitance qu’il conclurait éventuellement, une clause stipulant que :

1° le sous-traitant s’abstient de se rendre encore au lieu d’exécution du marché ou de poursuivre l’exécution du marché, lorsqu’une notification établie en exécution de l’article 49/2 du Code pénal social révèle que ce sous-traitant occupe un ressortissant d’un pays tiers en séjour illégal ;

2° le non-respect de l’obligation visée au point 1° est considéré comme un manquement grave dans le chef du sous-traitant, à la suite duquel l’entreprise est habilitée à résilier le contrat ;

3° le sous-traitant est tenu d’insérer, dans les contrats de sous-traitance, une clause analogue à celle visée aux points 1° et 2° et d’assurer que de telles clauses soient également insérées dans les contrats de sous-traitance ultérieurs.

## Rémunération due à ses travailleurs

Lorsque l’adjudicataire ou sous-traitant reçoit copie de la notification visée à l’article 49/1, alinéa 3, du Code pénal social, par laquelle il est informé d’un manquement grave à son obligation de payer dans les délais, à ses travailleurs, la rémunération à laquelle ceux-ci ont droit, cet adjudicataire ou sous-traitant s’abstient, avec effet immédiat, de se rendre encore au lieu d’exécution du marché ou de poursuivre l’exécution du marché, et ce jusqu’à ce qu’il présente la preuve à l’autorité adjudicatrice que les travailleurs concernés ont reçu l’intégralité de leur rémunération.

Il en va de même lorsque l’adjudicataire ou sous-traitant est informé :

- soit par l’adjudicataire ou par l’autorité adjudicatrice selon le cas de ce qu’ils ont reçu la notification visée à l’article 49/1, alinéa 1er, du Code pénal social, concernant cette entreprise ;

- soit via l’affichage prévu par l’article 35/4 de la loi du 12 avril 1965 relative à la protection de la rémunération des travailleurs.

Par ailleurs, l’adjudicataire ou sous-traitant est tenu d’insérer, dans les contrats de sous-traitance qu’il conclurait éventuellement, une clause stipulant que :

1° le sous-traitant s’abstient de se rendre encore au lieu d’exécution du marché ou de poursuivre l’exécution du marché, lorsqu’une notification établie en exécution de l’article 49/1 du Code pénal social révèle que ce sous-traitant manque gravement à son obligation de payer dans les délais, à ses travailleurs, la rémunération à laquelle ceux-ci ont droit ;

2° le non-respect de l’obligation visée au point 1° est considéré comme un manquement grave dans le chef du sous-traitant, à la suite duquel l’adjudicataire est habilité à résilier le contrat ;

3° le sous-traitant est tenu d’insérer, dans les contrats de sous-traitance, une clause analogue à celle visée aux points 1° et 2° et d’assurer que de telles clauses soient également insérées dans les contrats de sous-traitance ultérieurs.

## Protection des données

Les données personnelles collectées dans le cadre du marché public par l'attributaire du marché, ainsi que par ses sous-traitants, agissant en tant que responsables du traitement doivent être traitées conformément au Règlement général sur la protection des données (Règlement (UE) 2016/679 du Parlement Européen et Du Conseil du 27 avril 2016).

Dans ce cadre, l’attributaire et ses sous-traitants s’engagent à ce que les informations personnelles collectées soient utilisées uniquement pour l'exécution du marché, ou en exécution d'une obligation légale, ou avec l'accord explicite de l'adjudicateur. Le document NDA est joint en annexe au présent marché.

## Devoir de réserve et confidentialité

L’adjudicataire s’abstiendra, en toutes circonstances, de révéler le moindre renseignement concernant le marché ou IMIO et les bénéficiaires, sans l’approbation de IMIO. Cette obligation s’applique également à toute personne à laquelle on fait appel dans le cadre du présent marché. Les personnes mobilisées pour l’exécution du marché seront tenues de signer un engagement de confidentialité séparé à la demande de IMIO.

Il est renvoyé pour le surplus aux articles 19 à 23 de l’arrêté royal du 14 janvier 2013.

## Pénalités

Conformément à l’article 45, §1er de l’arrêté royal du 14 janvier 2013 établissant les règles générales d’exécution dans les marchés publics, le pouvoir adjudicateur est en mesure de réclamer une pénalité.

Les modalités de pénalités sont à définir par les pouvoirs adjudicateurs bénéficiaires, dans le cadre de leur(s) marché(s) subséquent(s).

## Compétence juridictionnelle et législation applicable

Le présent marché est exclusivement soumis au droit belge.

Tous les litiges relatifs à l’exécution de ce marché établissant la centrale d’achat et des marchés subséquents sont exclusivement tranchés par les tribunaux compétents de l’arrondissement judiciaire de Namur. La langue véhiculaire est le français.

IMIO n’est en aucun cas responsable des dommages causés à des personnes ou à des biens qui sont la conséquence directe ou indirecte des activités nécessaires à l’exécution de ce marché. L’adjudicataire garantit IMIO contre toute action en dommages et intérêts par des tiers à cet égard.

## Règlement Général de Protection des Données

* + 1. **Protection des données**

Informations relatives aux droits des soumissionnaires et adjudicataires en tant que personne concernée par le traitement des données personnelles dans le cadre du présent marché

En application du Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre

Circulation de ces données (le « RGPD »), l’intercommunale iMio, en tant que Pouvoir adjudicateur, est responsable du traitement des données des soumissionnaires au présent marché.

Les coordonnées du Pouvoir adjudicateur sont :

* IMIO
* Rue Léon Morel, 1,
* 5032 Isnes

Les coordonnées du Délégué à la protection des données du Pouvoir adjudicateur sont :

* iMio
* Jessie Maloteau
* vieprivee@imio.be

Dans le cadre du présent marché, les données du soumissionnaire ne sont traitées qu’aux fins de la gestion de la procédure d’attribution du présent marché et les données de l’adjudicateur sont traitées aux fins de la mise en œuvre du présent marché. En aucun cas, vos données ne sont traitées par le Pouvoir adjudicateur à des fins commerciales ou publicitaires ni transférées à des tiers qui utiliseraient ces données à de telles fins.

La durée de conservation de vos données n’excède pas la durée nécessaire au regard des finalités pour lesquelles les données sont traitées.

La passation du présent marché est conditionnée, en partie, à la transmission des données du soumissionnaire au pouvoir adjudicataire. La non-transmission de ces données peut avoir pour conséquence l’exclusion de la candidature du soumissionnaire en cause.

Dans le cadre de l’exécution du présent marché (en ce compris la phase précontractuelle), le Pouvoir adjudicateur peut être amené à recevoir ou à communiquer vos données à caractère personnel notamment aux destinataires suivants :

* Vous-même ;
* Des Pouvoirs locaux, Services publics fédéraux ou régionaux ;
* Des parties à une procédure administrative ou judiciaire qui implique l’intercommunale IMIO ;
* Des tiers dans le cadre d’obligations contractuelles.

Les données du soumissionnaire ne sont transmises à un pays tiers (hors UE) que dans la

Stricte nécessité de l’exercice des missions du pouvoir adjudicateur en tant qu’autorité publique ou lorsque une obligation légale ou conventionnelle l’impose.

Le soumissionnaire a les droits suivants, applicables dans les limites du RGPD :

* Droit d’accès à ses données ;
* Droit de rectifier ses données ;
* Droit à l’effacement de ses données ;
* Droit à la limitation du traitement de ses données ;
* Droit à la portabilité de ses données ;
* Droit de s’opposer au traitement de ses données.

Afin d’exercer ses droits, le soumissionnaire peut contacter le pouvoir adjudicataire en prenant directement contact avec notre Délégué à la protection des données.

Si le soumissionnaire estime que le pouvoir adjudicataire n’a pas respecté ses droits en matière de vie privée, il a la possibilité d’introduire une plainte auprès de l’autorité de protection des données belge :

* Autorité de protection des données
* Rue de la Presse, 35
* 1000 Bruxelles
* +32 274 48 00
* <https://www.autoriteprotectiondonnees.be/>
  + 1. **Obligations de l’adjudicataire en tant que sous-traitant du Pouvoir adjudicateur dans le cadre des traitements de données**

En application du Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (le « RGPD »), l’adjudicataire doit/peut être considéré comme sous-traitant pour le compte du Pouvoir adjudicateur.

Il en découle que l’adjudicataire s’engage à mettre en place toutes les garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que les traitements (éventuels) de données répondent aux exigences du RGPD et garantissent la protection des droits des personnes concernées par lesdits traitements.

À cet égard, l’adjudicataire s’engage à :

* Ne traiter les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel l’adjudicataire est soumis; dans ce cas, l’adjudicataire informe le Pouvoir adjudicateur de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;
* Veiller à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
* Prendre toutes les mesures appropriées afin de garantir la sécurité des traitements de données ;
* En tenant compte de la nature du traitement, aider le Pouvoir adjudicateur, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus ;
* Aider le Pouvoir adjudicateur à garantir le respect des obligations prévues par le RGPD (notamment en matière de sécurisation des données, d’analyse d’impact et de fuites de données) compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ;
* Selon le choix du responsable du traitement, supprimer toutes les données à caractère personnel ou les renvoyer au responsable du traitement au terme de la prestation de services relatifs au présent marché, et à détruire les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel ; et
* À mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits, y compris des inspections, par le Pouvoir adjudicateur ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

A cet égard, l’adjudicataire informe immédiatement le Pouvoir adjudicateur si, selon lui, une instruction constitue une violation du présent règlement ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

II.19.3 Sécurité

Il est demandé que le plus grand soin soit apporté par l’adjudicataire à la gestion de la sécurité informatique, tant matérielle (hardware) qu’immatérielle (software). La gestion de la sécurité informatique porte sur l’intégrité, la disponibilité et la confidentialité des données transportées mais aussi sur la protection contre les failles de sécurité et les infections de logiciels malveillants, tels que les virus, vers, portes dérobées, chevaux de Troie, logiciels espions et autres formes de logiciels malicieux.

L’adjudicataire prend toutes les mesures nécessaires, notamment de sécurité matérielle, afin d’éviter tout virus ou toute contamination de la structure informatique du Pouvoir adjudicateur tout au long de la durée du présent marché, qui seraient liés aux matériels et/ou aux prestations fournies par l’adjudicataire dans le cadre du présent marché.

En cas d’incident de sécurité (lui étant imputable ou non), l’adjudicataire s’engage à intervenir et à coopérer avec le Pouvoir adjudicateur pour rétablir le niveau de sécurité initial attendu, et à entreprendre tout ce qui est en son pouvoir pour éviter qu’un tel événement ne se reproduise dans le futur. Si l’incident de sécurité est imputable à l’adjudicataire ou à son matériel (y compris par le biais de ses sous-traitants), son intervention conformément au présent paragraphe est intégralement à sa charge.

## Centrale d’achat & Accord cadre

Le présent marché est passé sous forme d’une centrale d’achat, passant des activités d’achats centralisées sous la forme de marché, conformément aux articles 2, 6° et 7° b) et 47 de la loi du 17 juin 2016 sur les marchés publics.

Dans ce cadre, IMIO intervient en tant que pouvoir adjudicateur organisateur du marché. Chaque membre d’iMio est un pouvoir adjudicateur bénéficiaire du marché. Chaque « administration cliente » bénéficiaire du marché agira comme pouvoir adjudicateur.

Pour pouvoir bénéficier des marchés d’IMIO, « l’administration cliente » doit impérativement avoir marqué son intérêt et valablement décidé d’adhérer à la centrale d’achat. La liste des bénéficiaires ayant signé la convention à la date de la publication du présent Cahier spécial des charges est reprise en annexe D de ce cahier des charges. Cette liste de membres est disponible pour l’attributaire du marché sur demande auprès d’iMio, tout au long de l’exécution du marché.

Le prestataire s’engage à faire bénéficier, pendant toute la durée du marché, les adhérents à IMIO, des clauses et conditions reprises dans les documents du présent marché et, pour le surplus, dans l’offre de l’adjudicataire telle qu’approuvée par le pouvoir adjudicateur (prix, conditions de livraison, ...).

L’adhésion à la centrale d’achat « Cybersécurité » permet à « l’administration cliente » de commander des fournitures, logiciels et services en bénéficiant des conditions remises par les adjudicataires.

« L’administration cliente » bénéficie des marchés d’IMIO par simple commande.

D’un point de vue juridique, IMIO garantit à « l’administration cliente » que les dispositions prévues par la législation sur les marchés publics ont été respectées et que iMio est un pouvoir adjudicateur agissant sous forme de centrale au sens de l’article 2,6° de la loi 17 juin 2016.

La responsabilité de la sélection dans le catalogue de l’adjudicataire des fournitures ou services par commande est du ressort des membres bénéficiaires. IMIO agit en tant qu’intermédiaire via sa centrale de marché et n’est pas responsable d’une erreur de sélection dans les choix faits par le membre bénéficiaire.

Les membres bénéficiaires seront responsables des contrats qu’ils concluront avec l’attributaire retenu.

iMio ne supporte aucune responsabilité pour cette phase, cela n’empêche pas iMio de vérifier que les services et fournitures délivrées sont conformes aux services et fournitures fixés par ce marché public.

Lors d’une demande d’offre ou à la commande, l’adjudicataire devra vérifier que les configurations souhaitées sont cohérentes et adéquates aux attentes et situations propres de l’« administration cliente ».

La facturation des commandes de fournitures, logiciels ou services dans le cadre du présent marché seront facturés au « membre bénéficiaire » par l’adjudicataire.

Les termes fixés par l’accord cadre sont :

* Les experts proposés en réponse à cette procédure ouverte, participant aux missions d’analyse ;
* Les tarifs proposés dans l’inventaire ;
* Les méthodologies d’analyse .

## Limites de la centrale d’achat

La présente centrale d’achat est limitée aux pouvoirs adjudicateurs bénéficiaires (PAB), à savoir, des pouvoirs locaux wallons ayant marqué un intérêt préalablement au lancement du présent marché et listés en annexe D du présent cahier spécial des charges.

Les marchés subséquents sont commandés par les PAB au fur et à mesure des besoins de ses membres. Ces données ne sont pas un engagement ferme de commande de la part du pouvoir adjudicateur et de ses membres. Ces données constituent une information à l’attention des soumissionnaires.

Le montant cumulé maximal qui pourra être attribué dans le cadre de marchés subséquents fondés sur cet accord-cadre (tous lots confondus) est de 4.000.000 € TVAC. Une fois ce maximum atteint, aucun nouveau marché ne pourra plus être attribué via la centrale d’achat. La fin de la centrale d’achats ne porte pas préjudice à la poursuite de l’exécution des marchés subséquents en cours. La limite de la centrale d’achat est définie par les commandes des axes matériels, logiciels et services.

L’attention des soumissionnaires est attirée sur le fait que la conclusion de l’accord cadre n’entraîne aucune exclusivité dans leurs chefs, le PA se réservant donc le droit de satisfaire les besoins de ce présent marché par d’autres moyens (cfr absence d’exclusivité).

## Conditions d’accès

Pour pouvoir recourir à la centrale d’achat découlant de cette procédure ouverte, le Pouvoir local doit remplir 2 conditions :

* Avoir marqué son intérêt pour la centrale d’achat (Cfr Annexe D du présent cahier spécial des charges) ;
* Avoir décidé d’adhérer à la centrale d’achat (Cfr Annexe F du présent cahier spécial des charges). Sauf délégation, cette décision relève de l’organe législatif du pouvoir adjudicateur bénéficiaire (Conseil communal pour les Administrations Communales, Conseil de l’action sociale pour les CPAS, etc.) ;
* Avoir décidé de recourir à la centrale d’achat pour leur marché subséquent.

Les attributaires doivent s’assurer du respect de ces conditions pour établir une offre de prix basée sur cette centrale d’achat.

## Principe de la cascade - Ordre de consultation des attributaires

Dans le cadre des services auxiliaires d’achat, iMio consulte les attributaires à la demande du PAB, sur base de la date de démarrage souhaitée par le PAB.

Les attributaires seront contactés, dans l’ordre de classement résultant de cette procédure ouverte jusqu’à ce qu’un attributaire soit en mesure d’effectuer le marché subséquent sur base de la date de démarrage souhaitée par le PAB.

Afin de préserver le bon fonctionnement de la cascade, l’attributaire du marché consulté doit répondre endéans les 24h après la sollicitation, en l’absence de réponse, l’attributaire suivant dans la liste est contacté. Aucune omission ou manquement dans le chef de l’attributaire ne peut être invoqué pour justifier un manque à gagner et/ou d’autre(s) indemnisation(s) compensatoires se basant sur un quelconque manque à gagner. Il est donc fondamental que l’attributaire mette en place un canal de communication fonctionnel, efficace, et ne souffrant d’aucune carence en terme d’accès à la sollicitation.

Dès lors qu’un attributaire accepte la mission, il est mis en contact avec le PAB afin d’établir l’offre financière dans le cadre de cette centrale d’achat, s’en suit alors la procédure de commande décrite ci-après.

Tout soumissionnaire qui ne s’engage pas au respect des conditions fixées par le présent cahier spécial des charges, en ce qui concerne le fonctionnement de la cascade (délai de 24H pour répondre aux sollicitations d’iMio) verra son offre entachée d’irrégularité substantielle.

## Procédure de commande

La procédure de commande sera précisée lors du lancement de la centrale d’achat, toutefois, voici la procédure pressentie.

Pour chaque demande de devis, l’attributaire du marché doit :

* Vérifier l’adhésion du PAB à la centrale d’achat, pour ce faire, il obtient de la part du PAB la décision d’adhésion à la centrale d’achat Cybersécurité (modèle fourni en annexe F au présent cahier spécial des charges) ;
* Rencontrer le PAB et définir avec lui les éléments nécessaires à réalisation du projet (par éléments nécessaires, on entend toutes les prestations, logiciels et/ou matériels nécessaires) ;
* Informer iMio des :
  + Informations relatives au PAB (identification du PAB et délibération d’adhésion) ;
  + Nature de la mission demandée ;
  + Copie de l’offre réalisée en réponse à l’expression des besoins, cette offre doit spécifiquement faire référence à la centrale d’achat, et le lot correspondant.
* Transmettre au PAB l’offre réalisée en réponse à l’expression des besoins ;
* Obtenir la délibération d’attribution du marché subséquent, cette décision doit être basée sur la central d’achat.
* Transmettre cette délibération d’attribution à iMio.

Toute commande qui n’aura pas été obtenue en respectant ces étapes sera de facto considérée comme nulle et non-avenue.

## Procédure de réception des livraisons, implémentations et prestations

Lorsque l’attributaire du marché a terminé le travail tel que défini dans son offre de prix (Cfr procédure de commande), il doit :

* Obtenir le rapport de livraison signé par le pouvoir adjudicateur bénéficiaire (Annexe E du présent CSC) ;
* Facturer les services et équipements fournis ;
* Contrôler le paiement de la facture ;
* Transmettre à iMio ces éléments (rapport de livraison, facture émise et preuve de paiement)

## Moyens de contrôles

Ces éléments (liés à la commande et les facture/paiement) seront utilisés comme moyen de contrôle du respect des livrables et conditions de la centrale d’achat, et également pour l’octroi du subside régional relatif à la cybersécurité, il est donc fondamental que les fournisseurs respectent ces procédures et étapes. Un reporting général sera donc mis en œuvre, l’adjudicataire devra s’y conformer.

Tout soumissionnaire qui ne s’engage pas à respecter la procédure de commande et le reporting verra son offre déclarée irrégulière.

## Fonctionnaire dirigeant

L’exécution et la surveillance des fournitures et/ou services des marchés subséquents se déroulent sous le contrôle et la responsabilité du fonctionnaire dirigeant du pouvoir adjudicateur désigné par le membre bénéficiaire. Le fonctionnaire dirigeant peut se faire représenter par une personne physique. Dans ce cas, cette personne doit être désignée par le fonctionnaire dirigeant préalablement à l’attribution du marché subséquent.

Le fonctionnaire dirigeant est le seul compétent pour prendre des décisions en matière d’exécution. La personne désignée pour représentation permet un contact entre le pouvoir adjudicateur et l’adjudicataire. Elle n’a pas pouvoir de décision.

Mandats du fonctionnaire dirigeant et son représentant :

* Le fonctionnaire dirigeant est mandaté pour prendre toutes les décisions nécessaires, dans les limites imposées par le présent cahier spécial des charges, afin de veiller à la bonne exécution du contrat ;
* Toute promesse, modification ou accord qui diverge des conditions de ce Cahier spécial des Charges et qui n’est pas notifié par le pouvoir adjudicateur est à considérer comme nul par les deux parties ;
* Le fonctionnaire dirigeant peut déléguer tout ou partie de ses fonctions à un de ses délégués moyennant communication écrite aux participants concernés ;
* Le représentant du fonctionnaire dirigeant ne peut prescrire des services modificatifs ou supplémentaires quelconques sans l’accord écrit du Pouvoir adjudicateur.

Toutes communications et notifications que l’attributaire estime devoir faire concernant son marché sont faites, par écrit, au fonctionnaire dirigeant.

L’attributaire ne pourra se prévaloir du fait qu’une surveillance ou un contrôle a été exercé par le pouvoir adjudicateur ou son fonctionnaire dirigeant pour prétendre être dégagé de sa responsabilité si les travaux venaient à être refusés ultérieurement.

## Accord de non-divulgation

Il est essentiel que les soumissionnaires soient assurés du respect de la confidentialité entourant ce type d’information.

Le pouvoir adjudicateur s’engage à :

* Recevoir, à traiter et à conserver les informations confidentielles de manière confidentielle ;
* Ne pas utiliser les informations confidentielles, directement ou indirectement, pour un autre but que l’objet ou pour une éventuelle coopération entre les Parties (Pouvoir adjudicateur / Attributaire) ;
* Limiter la divulgation des informations confidentielles aux membres de son personnel et à ses partenaires qui ont véritablement besoin de les connaître et qui sont liés par une obligation de garder le secret par rapport aux Informations Confidentielles ;
* Nonobstant ce qui précède, le pouvoir adjudicateur peut divulguer, après autorisation écrite préalable de l’attributaire, des informations confidentielles à ses membres, mais uniquement dans la mesure où ces membres ont véritablement besoin de connaître ces informations confidentielles et seront, ainsi que leur personnel, tenus de maintenir ces informations confidentielles. Le pouvoir adjudicateur est responsable du respect du présent contrat par ses membres ;

Ne pas divulguer ces informations, en dehors des personnes autorisées et nécessitant l’accès à ces informations pour permettre le contrôle de la révision des prix.

# Description des exigences techniques

## Introduction

## Objectif

L’objectif du présent marché est de fournir un soutien professionnel aux Pouvoirs locaux pour la mise en place et le maintien de leurs programmes de cybersécurité dans la perspective de :

* Accroître la préparation et la résilience des entités essentielles des Pouvoirs locaux (telles que définies dans la proposition de l’arrêté du gouvernement relative à des mesures visant à assurer un niveau commun élevé de cybersécurité en Wallonie) et les services de cybersécurité qui aident l'organisation à répondre à un incident réel.
* Renforcer les capacités des Pouvoirs locaux en matière de cybersécurité, pour prévenir, traiter et répondre aux problèmes et menaces de cybersécurité.
* Fournir une assistance et des conseils aux Pouvoirs locaux sur les questions liées à la cybersécurité relevant de ses compétences telles que définies l’arrêté.

Les soumissionnaires doivent être en mesure de soutenir les capacités des Pouvoirs locaux pour tous les services soumissionnés auquel il prendra part. Le soutien à ces services doit être fourni selon les normes les plus élevées, de manière efficace et en temps voulu. Les soumissionnaires doivent également être en mesure de soutenir les Pouvoirs locaux dans la préparation et la gestion de ces services.

## Contexte

Le gouvernement wallon a lancé une initiative pour soutenir les Pouvoirs locaux dans leur volonté de se protéger contre les enjeux de la cybersécurité et de la cybercriminalité.

Pour répondre à ces besoins, le rôle de pouvoir adjudicateur pour différents marchés liés à cet enjeu a été confié à iMio. Le projet de mutualisation et de valorisation des actifs liés à la cybersécurité vise à mettre en place un "socle commun" de cyberdéfense en Wallonie, afin de permettre aux Pouvoirs locaux de préserver la continuité de leurs missions et la protection des données de leurs citoyens. Pour atteindre cet objectif, il est nécessaire de mettre en œuvre une approche globale qui inclut des solutions de matériel, de logiciel, et d'accompagnement adaptées aux besoins des Pouvoirs locaux. Cette procédure ouverte vise à sélectionner les fournisseurs qui proposeront les offres les plus adaptées et les plus compétitives pour répondre à ces enjeux.

De fait, iMio lance deux marchés se répartissant trois axes définis sur les caractéristiques des outils et services qui seront intégrés dans la centrale d’achat :

* Axe 1 : Accompagnement & formation
* Axe 2 : Matériel
* Axe 3 : Logiciel

Cette procédure ouverte concerne l’axe 1 «Accompagnement & formation »

L'évolution rapide du paysage des menaces, notamment l'augmentation du nombre de cyberattaques, exige des capacités solides dans le domaine de la cybersécurité pour garantir la résilience et la défense deson des exigences techniques a pour objectif de définir les critères techniques et fonctionnels que les produits et services proposés doivent respecter pour être retenus dans le cadre de cette procédure ouverte. Ces exigences sont essentielles pour garantir que les offres proposées répondent aux besoins et aux attentes des Pouvoirs locaux en matière de sécurité. Elles doivent donc être précises et détaillées afin de permettre aux soumissionnaires de présenter une offre qui réponde aux critères fixés.

Il est important de noter que ces exigences sont une condition sine qua non pour être retenu dans le cadre de cette procédure ouverte. Toute offre qui ne respecte pas ces exigences sera rejetée. Par conséquent, il est important de prendre le temps de bien comprendre et de respecter ces exigences afin de maximiser les chances de succès de votre offre.

Dans cette section, nous allons détailler les exigences techniques et fonctionnelles qui s'appliquent à chaque lot proposé dans cette procédure ouverte. Nous vous invitons donc à prendre le temps de lire attentivement ces exigences afin de vous assurer que votre offre répond aux critères fixés.

L'axe Accompagnement consiste en une assistance technique et une série de formations proposées par le soumissionnaire aux Pouvoirs locaux afin de les aider à mettre en œuvre les solutions proposées. Il peut inclure des services de support sur site, de formation, de mise en service ou de mise en œuvre de solutions. L'objectif de l'accompagnement est de permettre aux Pouvoirs locaux de bénéficier pleinement des avantages des solutions proposées et de les utiliser de manière optimale.

## Domaines d’expertises

Le niveau d'expertise attendu des experts est défini en fonction des spécificités techniques de chaque lot. Le profil qui n'atteint pas 75% des points d'expertise sera considéré comme irrégulière et sera exclue du marché, s’il s’agit du seul profil proposé, l’offre globale sera exclue du marché puisque ne rencontrant plus les critères de sélection qualitative.

Les experts doivent démontrer une solide formation académique dans le domaine de la cybersécurité, ainsi qu'une expérience pratique pertinente acquise lors de projets ou de stages. Ils doivent être capables de travailler en équipe et de s'adapter rapidement pour acquérir de nouvelles compétences techniques. Les connaissances et l'expérience des experts juniors seront évaluées en fonction des domaines d'expertise spécifiques à chaque lot.

Les experts seniors doivent justifier d'une expérience professionnelle approfondie d'au moins 7 ans dans le domaine de la cybersécurité, avec une expertise spécifique correspondant au lot concerné. Ils doivent démontrer leur maîtrise des normes et des meilleures pratiques, telles que l'ISO 27001, le NIS2 et le RGPD, ainsi que leur capacité à gérer des projets complexes et à fournir des conseils stratégiques en matière de cybersécurité. Les compétences et l'expérience des experts seniors seront également évaluées en fonction des domaines d'expertise spécifiques à chaque lot.

Il est essentiel que les soumissionnaires vérifient que les experts proposés possèdent les compétences techniques et l'expérience requises correspondant aux spécificités de chaque lot. Cela garantira la qualité et l'efficacité des services fournis dans le cadre du marché. Les détails des domaines d'expertise, ainsi que les critères d'évaluation, sont disponibles dans chaque lot du présent cahier spécial des charges.

La sélection des experts se fera en fonction des compétences démontrées dans leur curriculum vitae, qui devra attester de leur maîtrise des domaines d'expertise revendiqués. Les soumissionnaires sont invités à utiliser le tableau fourni dans l'Annexe C – Bordereau de réponse technique pour indiquer l'expérience professionnelle relative à chaque domaine d'expertise.

La combinaison de profils d'experts juniors et seniors est essentielle pour répondre aux exigences techniques spécifiques de chaque lot et assurer la qualité des services rendus.

## Glossaire

| Terme | Définition |
| --- | --- |
| ANSSI | L'Agence nationale de la sécurité des systèmes d'information est un service français. |
| ASD | Australian Signals Directorate |
| Audit de cybersécurité | Un audit de cybersécurité est un audit sur le niveau de sécurité de l'information dans une organisation afin de juger de la maturité de l’organisation. |
| CIS BENCHMARK | Normes de sécurité reconnues au niveau international pour la défense des systèmes et des données informatiques contre les cyberattaques. |
| CISSP | Certified Information Systems Security Professional |
| CSIRT | Une équipe d'intervention en cas d'incident de sécurité informatique (en anglais, Computer Security Incident Response Team ou CSIRT). |
| EBIOS | La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) est un outil complet de gestion des risques. |
| ICS | Information & Communication Services. |
| IOT | L'Internet des objets ou IdO (en anglais (the) Internet of Things ou IoT) |
| ISO | International Organization for Standardization (Organisation internationale de normalisation) |
| ISO 27001 | L'ISO/CEI 27001 est une norme internationale de sécurité des systèmes d'information de l'ISO et la CEI. |
| ISO 27002 | La norme ISO/CEI 27002 est une norme internationale concernant la sécurité de l'information. |
| ISO 27005 | La norme ISO/CEI 27005 décrit les grandes lignes d'une gestion des risques dans une perspective de mise en place d'un SMSI. |
| JIRA | Jira est un système de suivi de bugs, de gestion des incidents et de gestion de projets. |
| NIS | Directive “Network and Information System Security”. |
| NIS2 | Nouvelle directive “Network and Information System Security”. |
| NIST | National Institute of Standards and Technology |
| Pouvoir Locaux | Entités politiques subordonnées à l'Autorité fédérale et aux Régions, organisées sur le plan d'une province, d'une commune ou d'un district communal. |
| RGS | Le référentiel général de sécurité (RGS) est le cadre réglementaire permettant d’instaurer la confiance dans les échanges au sein de l’administration et avec les citoyens. |
| RSSI | Le responsable de la sécurité des systèmes d'information définit et développe la politique de sécurité de l'information de son entreprise. |
| SMSI | système de management de la sécurité de l'information. |
| TIC | Technologies de l'Information et de la Communication. |
| Vulnérabilités | Une vulnérabilité ou faille est une faiblesse dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système. |

## Exigences générales

* + 1. **Axe accompagnement**

L'axe "accompagnement" vise à fournir un soutien professionnel aux Pouvoirs locaux pour la mise en place et le maintien de leurs programmes de cybersécurité.

* + - 1. **Objectifs**

Cet axe soutient l’ensemble des services cybersécurité liés à l’accompagnement réglementaire (et assimilé) aux Pouvoirs locaux.

Les objectifs sont les suivants :

* Les services de cybersécurité contribueront à accroître la préparation et la résilience des entités essentielles des Pouvoirs locaux (telles que définies dans la proposition de l’arrêté du gouvernement relative à des mesures visant à assurer un niveau commun élevé de cybersécurité en Wallonie) et les services de cybersécurité qui aident l'organisation à répondre à un incident réel.
* Renforcer les capacités des Pouvoirs locaux en matière de cybersécurité, pour prévenir, traiter et répondre aux problèmes et menaces de cybersécurité.
* Fournir une assistance et des conseils aux Pouvoirs locaux de Wallonie sur les questions liées à la cybersécurité relevant de ses compétences telles que définies l’arrêté.
  + - 1. **Principales caractéristiques de cet axe**

Le soumissionnaire doit être en mesure de soutenir les capacités des Pouvoirs locaux pour tous les services soumissionnés auquel il prendra part. Le soutien à ces services doit être fourni selon les normes les plus élevées, de manière efficace et en temps voulu. Le soumissionnaire potentiel doit également être en mesure de soutenir les Pouvoirs locaux dans la préparation et la gestion de ces services.

Le soumissionnaire doit être capable de se conformer aux exigences et obligations des Pouvoirs locaux en matière de traitement et de protection de l'information, ainsi qu'en matière de responsabilité et de non-divulgation de l'information.

Le soumissionnaire doit être en mesure de satisfaire aux exigences spécifiques concernant la non-divulgation d'informations, si cela est requis dans une demande particulière.

Le contractant doit être capable de travailler ensemble (avec les conseils d’iMio et toute partie prenante jugée nécessaire) avec d'autres partenaires pertinents pour des demandes spécifiques (y compris d'autres soumissionnaires, des Pouvoirs locaux, etc.).

* + 1. **Rapports de missions et communication vers iMio (rapportage)**

En répondant à cette procédure ouverte, les soumissionnaires s’engagent à fournir des rapports de missions de qualité, à assurer une communication fluide avec iMio et à garantir la confidentialité et la sécurité des informations.

**Structure des rapports de missions :**

Les rapports de missions suivront une structure claire et cohérente comprenant une page de couverture, une table des matières, une introduction, les objectifs de la mission, les méthodologies utilisées, les résultats obtenus, les recommandations et un plan d'action. Des sections distinctes seront utilisées pour chaque aspect évalué afin de faciliter la lecture et la compréhension.

**Contenu détaillé des rapports de missions :**

Les rapports de missions fourniront une description détaillée des activités réalisées, des résultats obtenus, des problèmes identifiés et des recommandations spécifiques pour les résoudre. Des exemples concrets, des tableaux et des graphiques seront utilisés pour illustrer les résultats et rendre le rapport plus visuel et accessible.

**Échéancier des rapports de missions :**

En début de mission, un calendrier clair sera établi pour la soumission des rapports de missions, précisant les dates limites pour chaque étape du processus. Des délais raisonnables seront prévus pour permettre une analyse approfondie des résultats et la formulation de recommandations pertinentes.

**Présentation des rapports de missions :**

Les rapports de missions seront soigneusement structurés, faciles à lire et à comprendre. Une présentation visuelle attrayante avec une mise en page professionnelle, des graphiques et des schémas pertinents sera utilisée pour améliorer la lisibilité et la compréhension.

**Communication avec iMio :**

Pour assurer une communication efficace avec iMio, nous mettrons en place les mesures suivantes :

**Points de contact :**

Des points de contact clés seront désignés pour assurer une communication fluide et efficace avec iMio. Des responsables seront identifiés pour la coordination et la gestion des échanges avec iMio.

**Canal de communication :**

Des canaux de communication adaptés tels que les courriers électroniques, les réunions en ligne et les outils de gestion de projet collaboratifs seront utilisés. Une plateforme de partage d'informations centralisée sera établie pour faciliter la collaboration et le suivi des échanges (JIRA).

**Fréquence des échanges :**

Une fréquence régulière sera définie pour les échanges avec iMio, en tenant compte des besoins de suivi, de coordination et de communication des informations pertinentes. Des réunions périodiques seront prévues pour faire le point sur l'avancement des missions, discuter des problèmes éventuels et fournir des mises à jour sur les rapports de missions en cours.

**Gestion des problèmes et des changements :**

Un processus clair sera établi pour la gestion des problèmes et des changements, définissant les responsabilités, les étapes à suivre et les délais de résolution.

**Confidentialité et sécurité des informations :**

Nous accorderons une grande importance à la confidentialité et à la sécurité des informations liées aux projets. Les mesures suivantes seront prises :

**Politique de confidentialité / clause de non divulgation:**

Une politique de confidentialité et une clause de non divulgation stricte seront mises en place pour garantir la protection des informations sensibles. Les données seront traitées de manière confidentielle et ne seront accessibles qu'aux personnes autorisées.

**Sécurité des informations :**

Des mesures de sécurité appropriées seront mises en place pour protéger les informations contre tout accès non autorisé, toute divulgation ou toute altération. Les normes de sécurité de l'information seront respectées et les outils de sécurité appropriés seront utilisés pour protéger les données.

* + 1. **Profils nécessaires**
       1. **Gestionnaire du contrat**

IMIO désignera un point de contact pour gérer ce contrat et elle attend de chaque attributaire qu'il désigne un gestionnaire de contrat (et un remplaçant désigné) pour agir en tant que point de contact (unique) pour tous les besoins dans le cadre de cette procédure ouverte.

Le gestionnaire du contrat sera responsable de la gestion et de l'administration générale du projet, en ce compris la gestion des calendriers de rendez-vous, le bon suivi des demandes d’IMIO et la communication avec celle-ci, comme par exemple la facturation, etc.

Le(s) contractant(s) doit (doivent) fournir une adresse électronique et un numéro de téléphone vers lesquels toutes les communications doivent être acheminées.

Le contractant potentiel veillera à ce que des dispositions suffisantes soient prises pour que tous les congés/absences de son personnel soient couverts de manière adéquate, afin d'assurer la continuité des services faisant l'objet du contrat pendant tous les jours ouvrables normaux en Belgique, de 08 h 00 à 18 h 00 pendant les jours ouvrables (du lundi au vendredi) et en dehors des heures de bureau si nécessaire.

Toutes les communications avec l’ensemble des parties prenantes se feront en français, étant donné que c’est la langue de travail en Wallonie. Tous les livrables doivent être fournis en français également.

* + - 1. **Profil Experts (senior et junior)**

L'expert(s) en charge de la mission sera responsable de mener à bien les activités spécifiques du lot qui lui est assigné. Le travail sur site est préconisé afin de garantir la confidentialité des informations échangées. La langue utilisée pour les travaux, la rédaction des documents et la communication avec les parties prenantes est le français.

L'expert devra utiliser les outils et méthodologies spécifiques détaillé lors de la soumission (sauf accord préalable sur justification professionnelle) pour accomplir les tâches requises dans le cadre du lot.

Tous les documents et livrables résultant des activités de chaque lot devront être partagé auprès du pouvoir local concerné puis déposés dans le système de gestion de projets Jira, conformément aux échéances convenues. Des accès seront fournis à l'expert pour accéder au système et soumettre ses travaux. (A voir si iMio souhaite faire un suivi de toutes les activités).

La complétude, la qualité rédactionnelle, le respect des délais et la conformité aux normes et réglementations pertinentes, telles que ISO27001, NIS2 et RGPD, seront évalués pour chaque lot. L'expert devra s'assurer de remplir tous les critères mentionnés dans la partie "Obligations de Résultats" pour que les activités du lot soient considérées comme terminées avec succès.

## Descriptions des lots

## LOT A1 - Rédaction et accompagnement des politiques de sécurité

Un système de management de la sécurité de l'information (ISMS) est un cadre de gestion qui permet de définir comment une organisation protège ses données sensibles et ses systèmes d'information. En tant que Pouvoir local, il est important de se conformer aux réglementations et aux exigences en matière de sécurité de l'information, telles que le Règlement général sur la protection des données (RGPD), la norme ISO27001, NIS 2 et la Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. En établissant et en mettant en œuvre une politique de sécurité de l'information, vous pouvez garantir que vos données et vos systèmes sont protégés et que vous êtes en conformité avec les réglementations pertinentes.

Le soumissionnaire retenu aura également pour mission d'aider l'organisation à établir une feuille de route de sécurité qui définit les actions à entreprendre pour améliorer la sécurité des systèmes et des données de l'organisation, et de l'assister dans la mise en œuvre de ces mesures.

~~Il faudra également fournir aux Pouvoirs locaux wallons les moyens de gérer efficacement les incidents de cybersécurité.~~

## Objectifs du lot

* Rédaction de politiques de sécurité est de définir une stratégie claire et cohérente pour protéger les données et les systèmes de l'organisation, tout en respectant les réglementations et les exigences en matière de sécurité de l'information.
* Établir une feuille de route de sécurité qui définit les actions à entreprendre pour améliorer la sécurité des systèmes et des données de l’organisation ;
* Identifier les risques de sécurité existants et évaluer leur impact sur l’organisation ;
* Déterminer les priorités en matière de sécurité et mettre en place un plan d'action pour les aborder ;
* Assister l'organisation dans la mise en œuvre des mesures de sécurité recommandées dans la feuille de route de sécurité ;
* Fournir une assistance technique et une formation aux employés pour assurer la mise en œuvre efficace des mesures de sécurité, ainsi que sur les procédures de réponse aux incidents pour garantir que tout le personnel soit informé et préparé à agir rapidement et efficacement en cas d'incident ;
* Établir des indicateurs de performance pour suivre l'avancement des actions de sécurité et évaluer l'efficacité des mesures mises en place.
* L'intégration de ces procédures dans les systèmes de gestion de la sécurité de l'information (SGSI) pour une mise en œuvre efficace.
* ~~La mise en place des outils et des technologies pour détecter et répondre rapidement aux incidents, y compris la surveillance en temps réel et l'analyse des journaux.~~
* Le soutien de l'équipe de cybersécurité pour assister les Pouvoirs locaux wallons dans la gestion des incidents et dans les démarches de communication avec les autorités concernées

## Caractéristiques spécifiques du lot

Pour le lot de rédaction et accompagnement des politiques de sécurité pour les Pouvoirs locaux wallons, les soumissionnaires doivent proposer des services qui répondent aux exigences suivantes :

* Capacité à élaborer des politiques de sécurité qui répondent aux réglementations en vigueur et aux normes de l'industrie, telles que ISO 27001 et NIS 2 ;
* Connaissance approfondie des réglementations et des normes en matière de sécurité (par exemple, le RGPD ou les normes ISO 27001 et 27002) ;
* Mise en œuvre d'une approche personnalisée pour chaque Pouvoir local afin de tenir compte de leurs besoins spécifiques en matière de sécurité ;
* Prise en compte de l'ensemble des domaines de sécurité pertinents, tels que la sécurité physique, logique, des réseaux, des applications, des données et de la gestion de la continuité d'activité ;
* Fourniture de recommandations pratiques pour la mise en œuvre et le maintien des politiques de sécurité ;
* Capacité à travailler en étroite collaboration avec les équipes de sécurité et de gestion des Pouvoirs locaux pour s'assurer de la compréhension et de l'acceptation de ces politiques par tous les parties prenantes ;
* Mise à disposition de ressources de formation pour soutenir la mise en œuvre et la sensibilisation des politiques de sécurité ;
* Prise en compte de la réglementation en matière de sécurité et de protection de données en vigueur, notamment le RGPD ;
* Élaboration de politiques de sécurité adaptées aux besoins et aux ressources du Pouvoir local ;
* Mise en place d'un processus de gestion de la sécurité en ligne avec les meilleures pratiques de l'industrie ;
* Formalisation de procédures de gestion des incidents de sécurité et de gestion des risques ;
* Mise en place de mécanismes de surveillance et de contrôle pour s'assurer du respect des politiques de sécurité établies ;
* Mise à disposition de supports de formation pour sensibiliser les utilisateurs aux bonnes pratiques de sécurité ;
* Assistance à la mise en œuvre des politiques de sécurité et suivi de leur mise en œuvre.
* Capacité à identifier et évaluer les risques de sécurité existants, et à proposer des solutions adaptées pour les atténuer ;
* Expérience de la formation et de l'assistance technique aux employés pour assurer la mise en œuvre efficace des mesures de sécurité ;
* Capacité à établir des indicateurs de performance pour suivre l'avancement des actions de sécurité et évaluer l'efficacité des mesures mises en place ;
* Disponibilité pour fournir un support continu et une assistance technique aux employés de l'organisation pour toute question relative à la sécurité.
* La mise en place d'un plan de réponse aux incidents qui décrit les procédures à suivre pour identifier, analyser et gérer les incidents de sécurité de l'information. Ce plan devra inclure des procédures pour la détection d'incidents, la classification des incidents, la notification des parties prenantes, l'analyse de l'incident, la réponse à l'incident et le suivi après l'incident ;
* La formation des employés des Pouvoirs locaux sur les procédures de réponse aux incidents pour garantir que tout le personnel est informé et préparé à agir rapidement et efficacement en cas d'incident. Les formations devront inclure des scénarios d'incidents réels et des exercices pour entraîner les employés aux procédures de réponse aux incidents ;
* L'intégration de ces procédures dans les systèmes de gestion de la sécurité de l'information (SGSI) pour une mise en œuvre efficace. Les outils de gestion de la sécurité devront être configurés pour automatiser les tâches de réponse aux incidents et pour fournir des informations en temps réel sur l'état des incidents ;
* ~~La mise en place des outils et des technologies pour détecter et répondre rapidement aux incidents, y compris la surveillance en temps réel et l'analyse des journaux. Il est attendu que le prestataire fournisse des outils pour la détection des intrusions, la détection des anomalies et la détection des menaces avancées ;~~
* ~~Le soutien de l'équipe de cybersécurité pour assister les Pouvoirs locaux wallons dans la gestion des incidents et dans les démarches de communication avec les autorités concernées. Cela inclura un soutien 24/7 pour la gestion des incidents et une assistance pour les déclarations et les communications requises par les autorités réglementaires ;~~
* ~~La mise en place d'une plateforme de gestion des incidents pour centraliser la gestion des incidents et faciliter la communication entre les différentes équipes impliquées ;~~
* La mise en place d'une procédure de "isolement" pour limiter les impacts d'un incident et empêcher sa propagation ;
* La mise en place d'une procédure de "récupération" pour récupérer les systèmes et les données affectés par l'incident ;
* La mise en place d'une procédure de "leçons apprises" pour identifier les causes de l'incident et mettre en place des mesures pour éviter les récurrences ;
* La mise en place d'un processus de rapport pour informer les autorités réglementaires et les parties prenantes de l'incident et de ses résultats ;
* La mise en place d'un plan de continuité d'activité pour garantir la continuité des opérations des Pouvoirs locaux en cas d'incident majeur.

## Spécificités techniques

Le Pouvoir local est confronté à de nombreuses réglementations et exigences en matière de sécurité de l'information. Afin de s'assurer que les politiques de sécurité sont adéquates et respectent ces exigences, il est essentiel de mettre en place un système de gestion de la sécurité de l'information (ISMS) :

* Capacité à évaluer les exigences et réglementations en matière de sécurité de l'information applicables au Pouvoir local ;
* Connaissance approfondie des meilleures pratiques en matière de rédaction de politiques de sécurité de l’information ;
* Capacité à fournir des recommandations sur les contrôles de sécurité à mettre en place pour protéger les actifs de l’organisation ;
* Expérience dans la rédaction de politiques de sécurité pour des organisations similaires au Pouvoir local ;
* Capacité à fournir un support continu pour la mise à jour et le suivi des politiques de sécurité de l’information ;
* Connaissance approfondie des réglementations et normes en matière de sécurité de l'information, telles que le RGPD, ISO 27001, NIS 2, etc. ;
* Expérience de la rédaction et de la mise en œuvre de politiques de sécurité dans des environnements similaires, tels que des Pouvoirs locaux ou des gouvernements locaux ;
* Capacité à adapter les politiques de sécurité aux besoins spécifiques du Pouvoir local, en tenant compte de sa taille, de son secteur d'activité et de ses obligations réglementaires ;
* Expérience de la communication et de la sensibilisation des agents aux politiques de sécurité, afin d'assurer une adhésion efficace de l'ensemble de l'organisation.
* Connaissance de l'intégration des politiques de sécurité dans les processus de gestion de l'organisation et dans les systèmes informatiques ;
* Capacité à évaluer et à mettre à jour régulièrement les politiques de sécurité pour tenir compte des changements dans l'environnement de sécurité

## Domaines d’expertises

Pour garantir la sécurité de leurs systèmes d'information, les Pouvoirs locaux sont tenus de mettre en place des politiques de sécurité claires et efficaces. Il est essentiel que les soumissionnaires pour le lot de rédaction des politiques de sécurité possèdent une expertise approfondie dans ce domaine afin de garantir la qualité et l'efficacité des politiques produites :

* Connaissance des réglementations et normes en matière de sécurité de l'information, telles que ISO 27001 et GDPR ;
* Expérience de la rédaction de politiques de sécurité pour les organisations publiques et/ou de grande taille ;
* Connaissance des meilleures pratiques en matière de gestion de la sécurité de l'information, y compris la mise en place de contrôles de sécurité, la gestion des risques et la gestion de la sécurité des données ;
* Compétences en matière de communication et de présentation pour assurer la compréhension et l'adoption des politiques de sécurité par les agents et les parties prenantes de l’organisation ;
* Connaissance approfondie des réglementations et législations en matière de sécurité des systèmes d'information, telles que le RGPD, la loi relative à la protection de la vie privée, etc. ;
* Expérience dans la mise en place et la gestion de systèmes de gestion de la sécurité de l'information (ISMS) et de la certification ISO 27001 ;
* Bonne compréhension des besoins et des enjeux de sécurité des Pouvoirs locaux, ainsi que de leurs structures et de leurs processus opérationnels ;
* Capacité à établir une stratégie de sécurité adaptée aux besoins et aux contraintes des Pouvoirs locaux, en prenant en compte leurs objectifs et leurs ressources ;
* Connaissance de l'ensemble des domaines de la sécurité de l'information, tels que la sécurité des réseaux, de la donnée, de l'application, de l'accès, de l'identité, etc. ;
* Capacité à communiquer de manière claire et concise sur les politiques de sécurité et à les adapter aux différents publics cibles (personnels, utilisateurs, autorités, etc.).

## Rapports et documentations

Pour assurer l'efficacité et la pertinence de la rédaction des politiques de sécurité pour les Pouvoirs locaux wallons, il est important que les soumissionnaires présentent une documentation complète et précise de leur processus de travail et de leur expertise dans ce domaine. Cela permettra de s'assurer que les soumissionnaires ont les compétences et l'expérience nécessaires pour répondre aux exigences spécifiques de chaque Pouvoir local et pourra leur fournir une politique de sécurité adaptée à leurs besoins.

Documents requis :

* Un CV détaillé du ou des responsables du projet, mettant en avant leur formation et leur expérience en matière de rédaction de politiques de sécurité ;
* Des exemples de politiques de sécurité précédemment rédigées par le soumissionnaire, ainsi que des témoignages de clients satisfaits ;
* Un descriptif détaillé du processus de travail du soumissionnaire pour la rédaction de politiques de sécurité, incluant les étapes clés et les méthodologies utilisées ;
* Des informations sur les outils et les technologies utilisés par le soumissionnaire pour la rédaction et la gestion des politiques de sécurité ;
* Une liste des réglementations et normes de sécurité auxquelles les politiques de sécurité devront être conformes ;
* Des preuves de la capacité du soumissionnaire à travailler en collaboration avec les équipes de sécurité et de gestion des Pouvoirs locaux pour établir des politiques de sécurité adaptées aux besoins de chaque organisation ;
* Des évaluations de la conformité aux réglementations et normes de sécurité réalisées précédemment pour d'autres clients, avec une description des résultats obtenus et des recommandations faites pour améliorer la sécurité.

## Obligation de résultat

Le lot de rédaction des politiques de sécurité a pour objectif de fournir aux Pouvoirs locaux wallons des politiques de sécurité claires, complètes et adaptées à leurs besoins. Pour atteindre cet objectif, les soumissionnaires doivent être en mesure de démontrer leur capacité à fournir les résultats suivants :

* Mise en place d'un processus de rédaction de politiques de sécurité adapté aux besoins des Pouvoirs locaux wallons et conforme aux réglementations en vigueur ;
* Rédaction de politiques de sécurité claires, complètes et adaptées aux besoins des Pouvoirs locaux wallons ;
* Mise à disposition d'outils de suivi et de rapport pour mesurer l'efficacité des politiques de sécurité ;
* Mise en place de processus de mise à jour régulière des politiques de sécurité pour garantir leur pertinence et leur conformité aux réglementations en vigueur ;
* Mettre en place une politique de sécurité adaptée aux exigences légales et réglementaires en vigueur ;
* Assurer la mise à jour régulière de la politique de sécurité en fonction de l'évolution de l'environnement légal et réglementaire ;
* Garantir la diffusion et la sensibilisation des politiques de sécurité auprès de tous les agents ;
* Mettre en place des procédures de gestion des incidents de sécurité et assurer leur mise à jour régulière ;
* Assurer la mise en place de mesures de contrôle et de suivi de la conformité à la politique de sécurité ;
* Fournir des rapports périodiques sur l'état de mise en œuvre de la politique de sécurité et sur les éventuels incidents de sécurité survenus.

## Description du contenu du forfait attendu

L'établissement d'un forfait de rédaction (Cfr bordereau de prix) de politiques de sécurité pour une organisation publique nécessite un ensemble spécifique de tâches. Voici un exemple de ce que pourrait inclure un tel ensemble de tâches :

* Analyse des exigences : Comprendre le contexte spécifique de l'organisation publique, y compris son environnement réglementaire, ses objectifs stratégiques, ses risques de sécurité spécifiques, etc.
* Évaluation des risques : Mener une évaluation approfondie des risques pour identifier les vulnérabilités de sécurité et évaluer l'impact potentiel de chaque menace sur chaque actif concerné.
* Élaboration de la structure des politiques : Créer une structure pour les politiques qui couvrira tous les domaines nécessaires, en accord avec les réglementations en vigueur comme défini dans l’analyse initiale.
* Rédaction des politiques : Rédiger les politiques de sécurité individuelles, y compris les détails sur les contrôles de sécurité, les responsabilités, les procédures d'audit et de conformité, etc.
* Consultation et approbation : Fournir un processus de consultation pour les parties prenantes clés de l'organisation pour qu'elles puissent examiner les politiques et donner leur approbation.
* Formation et sensibilisation : Développer et déployer des programmes de formation et de sensibilisation pour s'assurer que le personnel de l'organisation comprend les politiques et sait comment les appliquer.

## Lot A2 - Évaluation des vulnérabilités et « pen tests »

## Objectifs du lot

Le lot "Évaluation des vulnérabilités" a pour objectif principal d'aider les Pouvoirs locaux wallons à identifier les vulnérabilités potentielles dans leurs systèmes d'information et à évaluer les risques associés à ces vulnérabilités. Les objectifs spécifiques de ce lot sont les suivants :

* Identifier les vulnérabilités dans les systèmes d'information des Pouvoirs locaux, y compris les systèmes réseau, les systèmes d'application, les systèmes de stockage de données et les systèmes de sécurité ;
* Évaluer les risques associés à ces vulnérabilités en utilisant des méthodologies éprouvées et des outils de test de vulnérabilité ;
* Fournir un rapport détaillé des vulnérabilités identifiées et des risques associés, avec des recommandations pour remédier aux vulnérabilités et réduire les risques ;
* Offrir des services de suivi pour vérifier que les vulnérabilités identifiées ont été corrigées et pour évaluer de nouveau les risques après la mise en place des remèdes ;
* Offrir une formation pour les employés des Pouvoirs locaux pour les aider à comprendre les vulnérabilités et à s'engager dans des pratiques de sécurité efficaces.

Les projets proposés doivent être innovants, en utilisant les dernières technologies, les outils et les méthodes d'évaluation de vulnérabilités pour identifier les vulnérabilités cachées et évaluer les risques de manière précise. Les soumissionnaires doivent également s'engager à fournir un soutien continu après la livraison des projets pour assurer que les vulnérabilités sont correctement gérées et que les risques sont continuellement évalués.

## Caractéristiques spécifiques du lot

La caractéristique spécifique de ce lot est de fournir une évaluation complète et précise des vulnérabilités dans les systèmes d'information des Pouvoirs locaux wallons. En ce sens :

* Présenter des méthodologies et des outils innovants pour identifier les vulnérabilités cachées dans les systèmes d'information des Pouvoirs locaux ;
* Évaluer les risques associés à ces vulnérabilités de manière précise et en utilisant des outils de test de vulnérabilité éprouvés ;
* Fournir un rapport détaillé des vulnérabilités identifiées et des risques associés, avec des recommandations pour remédier aux vulnérabilités et réduire les risques ;
* Offrir des services de suivi pour vérifier que les vulnérabilités identifiées ont été corrigées et pour évaluer de nouveau les risques après la mise en place des remèdes ;
* Offrir une formation pour les employés des Pouvoirs locaux pour les aider à comprendre les vulnérabilités et à s'engager dans des pratiques de sécurité efficaces ;
* Présenter des méthodologies et des outils pour évaluer les vulnérabilités dans les environnements cloud, y compris les plateformes AWS, Azure, O365, etc ;
* Fournir des services de gestion de vulnérabilités pour aider les Pouvoirs locaux à suivre et à gérer les vulnérabilités identifiées au fil du temps.

## Spécificités techniques

La spécificité technique de ce lot est de fournir une évaluation complète et précise des vulnérabilités dans les systèmes d'information des Pouvoirs locaux wallons. Les soumissionnaires doivent présenter des méthodologies et des outils innovants, utiliser les dernières technologies et respecter les normes ISO 27001, NIS 2 :

* Présenter les outils de détection de vulnérabilités utilisés (ex: Nessus, Qualys, Nmap, etc.) ;
* Capacité à identifier les vulnérabilités dans les systèmes d'information des Pouvoirs locaux, y compris les systèmes cloud ;
* Capacité à utiliser des outils automatisés et manuels pour évaluer les vulnérabilités ;
* Capacité à évaluer les risques associés aux vulnérabilités identifiées et à fournir des recommandations pour remédier aux vulnérabilités et réduire les risques ;
* Capacité à fournir un suivi pour vérifier que les vulnérabilités identifiées ont été corrigées et pour évaluer de nouveau les risques après la mise en place des remèdes ;
* Capacité à fournir une formation pour les employés des Pouvoirs locaux pour les aider à comprendre les vulnérabilités et à s'engager dans des pratiques de sécurité efficaces ;
* Capacité à utiliser les normes ISO 27001 et NIS 2 pour identifier les vulnérabilités dans les systèmes d'information des Pouvoirs locaux ;
* Capacité à fournir des rapports de vulnérabilités détaillés et des recommandations pour remédier aux vulnérabilités et réduire les risques ;
* Capacité à offrir des services de test d'intrusion pour vérifier la résistance des systèmes aux attaques réelles ;
* Capacité à offrir des services de gestion de vulnérabilités pour aider les Pouvoirs locaux à suivre et à gérer les vulnérabilités identifiées au fil du temp ;
* Capacité à offrir des services de gestion de la réponse aux incidents pour aider les Pouvoirs locaux à planifier et à gérer efficacement les incidents de sécurité.

## Domaines d’expertise

Afin de s’assurer d’un niveau d’excellence de la part des soumissionnaires, les domaines d’expertises suivants seront attendus :

* Connaissance approfondie des normes et des réglementations en matière de sécurité de l'information, comme ISO 27001 et NIS 2.
* Expérience de la mise en place de programmes de gestion des vulnérabilités pour les entreprises ou les organisations publiques.
* Expérience de la réalisation d'évaluations de vulnérabilités pour les systèmes d'information, les systèmes cloud, les systèmes IoT et les systèmes industriels.
* Expérience dans l'utilisation des outils de détection de vulnérabilités automatisés et manuels.
* Expérience en matière de sécurité des systèmes cloud (AWS, Azure, O365, etc.).
* Expérience dans la formation des employés à la sécurité de l'information.
* Expérience dans la mise en place de programmes de test d'intrusion et d'évaluation des risques.
* Expérience dans la gestion de la réponse aux incidents de sécurité.
* Certifications ou accréditations pertinents en matière de sécurité de l'information.
* Expérience dans la fourniture de rapports et de recommandations détaillées pour remédier aux vulnérabilités et réduire les risques.

## Rapports et documentations

Pour le lot "Évaluation des vulnérabilités", voici quelques types de rapports et de documentations à fournir :

* Des rapports de vulnérabilités détaillés qui décrivent les vulnérabilités identifiées, leur impact potentiel, leur priorité et les recommandations pour les remédier ;
* Des plans de gestion des vulnérabilités qui décrivent les étapes à suivre pour suivre et gérer les vulnérabilités identifiées au fil du temps ;
* Des rapports de test d'intrusion qui décrivent les méthodes utilisées pour tester la résistance des systèmes aux attaques réelles, les résultats obtenus et les recommandations pour remédier aux vulnérabilités identifiées ;
* Des documents de garantie de service qui décrivent les engagements en matière de service après-vente et de support technique ;
* Des informations sur les certifications et les accréditations des soumissionnaires en matière de sécurité de l'information ;
* Des références clients pour vérifier l'expérience et la compétence des soumissionnaires dans les domaines pertinents.

## Obligation de résultat

Les obligations de résultats suivantes sont attendues des soumissionnaires pour garantir une protection efficace des Pouvoirs locaux wallons et une gestion efficace des vulnérabilités:

* Obligation de fournir des rapports de vulnérabilités détaillés et des plans de gestion des vulnérabilités dans les délais convenus ;
* Obligation de remédier aux vulnérabilités critiques dans un délai défini ;
* Obligation de fournir des services de test d'intrusion pour vérifier la résistance des systèmes aux attaques réelles ;
* Obligation de fournir des services de gestion de la réponse aux incidents pour aider les Pouvoirs locaux à planifier et à gérer efficacement les incidents de sécurité ;
* Obligation de respecter les normes ISO 27001 et NIS 2 pour identifier les vulnérabilités dans les systèmes d'information des Pouvoirs locaux ;
* Obligation de respecter les engagements en matière de service après-vente et de support technique ;
* Obligation de maintenir la confidentialité et la sécurité des données des Pouvoirs locaux ;
* Obligation de fournir des formations pour les employés des Pouvoirs locaux sur les meilleures pratiques en matière de gestion des vulnérabilités ;
* Obligation de fournir des mises à jour régulières sur l'avancement des projets et de résoudre les problèmes dans les délais convenus.

## Lot A3 - Campagne de test de phishing/vishing/social engineering

## Objectifs du lot

Le lot sur les campagnes de prévention et de formation aux phishing, vishing et social engineering a pour objectif de renforcer la résilience des Pouvoirs locaux face aux tentatives de cyber intrusion par ces méthodes et plus spécifiquement la résilience des agents œuvrant en leurs seins. Pour atteindre cet objectif, ce lot doit inclure les éléments suivants :

* Des campagnes de sensibilisation auprès des agents des agents des Pouvoirs locaux afin de les informer sur les risques liés aux tentatives de phishing, vishing et social engineering et sur les bonnes pratiques pour les éviter ;
* Des campagnes de test de phishing et de vishing afin de mesurer la vulnérabilité des agents aux tentatives de cyber intrusion et de mettre en place des actions de correction en cas de résultats insuffisants ;
* Des formations sur les bonnes pratiques pour éviter les tentatives de phishing, vishing et social engineering, ainsi que sur les techniques utilisées par les cybercriminels pour mener ces attaques ;
* La mise à disposition d'une base de données de connaissances sur les techniques de phishing, vishing et social engineering et sur les moyens de les prévenir ;
* Améliorer la compréhension des pratiques de sécurité appropriées pour protéger contre ces menaces ;
* Mettre en place un programme de formation continue pour maintenir et améliorer les compétences en matière de sécurité des utilisateurs ;
* Evaluer l'efficacité des campagnes de formation et de prévention en utilisant des indicateurs de performance clés ;
* Encourager la collaboration et le partage d'informations sur les menaces et les bonnes pratiques de sécurité auprès des utilisateur ;
* Réduire les taux de réussite des campagnes de phishing, vishing et social engineering en utilisant des méthodes de formation interactives et mémorables ;
* Favoriser l'adoption de comportements sécurisés pour éviter les erreurs qui peuvent mener à des compromissions.

En somme, l'objectif de ce lot est de renforcer la capacité des Pouvoirs locaux à se défendre contre les tentatives de cyber intrusion par phishing, vishing et social engineering, grâce à une sensibilisation et une formation adaptée, ainsi qu'à une prise de conscience accrue des risques liés à ces techniques.

## Caractéristiques spécifiques du lot

Les caractéristiques spécifiques du lot sont à considérer comme étant les caractéristiques minimales à fournir :

* Objectifs de la campagne : la campagne devra avoir pour objectif de sensibiliser les agents aux différentes techniques de phishing, vishing et social engineering, afin qu'ils puissent les détecter et y résister. Elle devra également viser à renforcer la culture de sécurité de l'entreprise en promouvant une meilleure compréhension des enjeux de la cybersécurité et des moyens de se protéger contre les attaques ;
* Contenu de la formation : le lot devra prévoir une formation adaptée aux besoins et aux compétences de l'audience cible, qui pourra être dispensée sous forme de modules en présentiel, de webinaires ou de supports de formation en ligne. La formation devra couvrir l'ensemble des techniques de phishing, vishing et social engineering, ainsi que les bonnes pratiques pour les prévenir et les détecter ;
* Méthodes pédagogiques : la formation devra utiliser des méthodes pédagogiques adaptées pour favoriser l'acquisition des connaissances et la mémorisation des informations par les participants. Cela pourra inclure des exercices pratiques, des cas d'étude, des quizz ou tout autre support pédagogique permettant de rendre la formation interactive et participative ;
* Modalités de suivi et d'évaluation : le lot devra prévoir des modalités de suivi et d'évaluation de la formation, afin de s'assurer de sa pertinence et de son efficacité. Cela pourra inclure des enquêtes de satisfaction auprès des participants, des évaluations en cours et en fin de formation, ou tout autre outil permettant de mesurer l'impact de la formation sur les compétences et les pratiques des agents ;
* Contenu de la formation : le soumissionnaire devra fournir une liste non exhaustive des sujets abordées lors des formations ;
* Responsabilité de la formation : le soumissionnaire devra préciser qui sera chargé de la mise en œuvre de la formation, et quelles seront les compétences et les expériences de cette personne en matière de cybersécurité et de formation. Il devra également préciser comment seront garanties la qualité et la pertinence de la formation, et comment seront assurés le suivi et l'évaluation de celle-ci.

## Spécificités techniques

Pour ce qui est des spécificités techniques du marché, il est important de prendre en compte les exigences suivantes :

* La plateforme de formation doit être accessible via un navigateur web et être compatible avec les principaux systèmes d'exploitation (Windows, MacOs, Linux, etc.). La plateforme doit être accessible également via téléphone mobile et offrir une expérience équivalente à un environnement sur ordinateur.
* La plateforme doit être capable de gérer les différents niveaux de privilèges et de droits d'accès des utilisateurs, ainsi que leur gestion des identifiants et mots de passe. Ces droits doivent être gérables par le Pouvoir local via une interface dédiée.
* La plateforme doit être sécurisée et protégée contre les attaques de type DDoS et autres menaces en ligne.
* Le soumissionnaire doit fournir une documentation détaillée sur l'installation, la configuration et l'utilisation de la plateforme de formation.
* Le soumissionnaire doit également proposer une assistance technique pour la mise en place et le déploiement de la plateforme, ainsi que pour son utilisation quotidienne par les utilisateurs.
* La possibilité de personnaliser les campagnes de formation et de prévention pour chaque Pouvoir local, en fonction de leurs besoins et de leur niveau de maturité en matière de cybersécurité
* L'intégration de scénarios réalistes dans les campagnes de formation, afin de sensibiliser les utilisateurs à la variété des menaces qui peuvent être rencontrées
* L'utilisation de plateformes de formation en ligne accessibles depuis n'importe quel appareil et connecté à internet
* L'inclusion de tests et d'évaluations pour mesurer l'efficacité de la formation
* La fourniture de support technique et de ressources pour aider les Pouvoirs locaux à mettre en place et à gérer les campagnes de formation et de prévention.

## Domaines d’expertises

Les experts dans le domaine des campagnes de phishing, vishing et social engineering doivent démontrer leur expertise dans la sensibilisation, la détection et la prévention des attaques de cyberintrusion:

* Connaissance approfondie des techniques de phishing, vishing et social engineering pour comprendre les méthodes employées par les cybercriminels.
* Expérience en conception et réalisation de campagnes de sensibilisation pour informer les utilisateurs sur les risques et les bonnes pratiques de prévention.
* Compétences en évaluation de la vulnérabilité aux attaques de phishing pour conduire des campagnes de test et évaluer la réaction des utilisateurs.
* Connaissance des bonnes pratiques de sécurité pour prévenir les attaques de phishing, vishing et social engineering et conseiller les utilisateurs sur les mesures de protection à adopter.
* Expérience en formation sur les bonnes pratiques de sécurité pour sensibiliser les utilisateurs aux risques et leur enseigner les actions à prendre pour se protéger.
* Connaissance des outils de détection et de prévention des attaques de phishing, vishing et social engineering pour recommander et mettre en œuvre des solutions technologiques de protection.
* Évaluation de l'efficacité des campagnes de formation et de prévention pour mesurer l'engagement des utilisateurs et l'impact des mesures de sensibilisation.
* Maîtrise des techniques de collecte d'informations et d'analyse des incidents de phishing, vishing et social engineering pour identifier les schémas d'attaque et prendre des mesures correctives.
* Connaissance des réglementations et des normes relatives à la protection des données personnelles, telles que le RGPD, pour garantir la conformité lors de la collecte et du traitement des données.
* Capacité à élaborer des rapports détaillés sur les campagnes de phishing, vishing et social engineering, incluant des recommandations pour améliorer la sécurité et renforcer la résilience des utilisateurs face à ces attaques.

## Rapports et documentations

Le soumissionnaire devra être en mesure de fournir des rapports détaillés et des documents de suivi pour chaque campagne de prévention et de formation menée. Ces documents devront inclure les informations suivantes :

* Le nombre de personnes formées et les détails de leur formation (thèmes abordés, durée, etc.) ;
* Les résultats de chaque campagne (taux de clics sur les liens malveillants, taux de réussite aux tests de sensibilisation, etc.) ;
* Des recommandations pour améliorer la protection contre les phishings, vishing et autres types d'attaques de social engineering ;
* Le soumissionnaire devra également être en mesure de fournir un plan de continuité pour chaque campagne de formation, afin de s'assurer que les connaissances acquises par les utilisateurs sont maintenues et renforcées sur le long terme. Enfin, il devra être en mesure de fournir des supports de formation adaptés aux besoins des utilisateurs, tels que des guides de sensibilisation, des présentations PowerPoint, etc. ;
* Des exemples concrets d'attaques réussies et échouées, ainsi que les leçons à tirer de ces cas ;
* Une analyse des tendances et des menaces émergentes dans ce domaine ;
* Des études de cas ou des cas pratiques pour illustrer les enjeux de la cybersécurité pour les Pouvoirs locaux ;
* Des illustrations pour intégrer la prévention du phishing, du vishing et du social engineering dans la stratégie de cybersécurité globale des Pouvoirs locaux.

## Obligation de résultat

Pour le lot de campagnes de prévention et de formation aux phishing, vishing et social engineering, le soumissionnaire doit s'engager à fournir des résultats concrets et mesurables. Ces résultats peuvent inclure, mais ne sont pas limités à :

* Un niveau de sensibilisation élevé et une bonne compréhension des techniques d'attaque parmi les utilisateurs cibles de ces campagnes ;
* Des indicateurs de performance clairs et précis pour mesurer l'efficacité des campagnes de prévention et de formation ;
* Des données sur les attaques réussies et échouées, ainsi que sur les utilisateurs qui ont réagi correctement ou incorrectement aux tentatives d'attaque ;
* Le soumissionnaire devra également présenter une stratégie de suivi et de surveillance pour s'assurer que les résultats obtenus sont maintenus sur la durée de l'accord. Enfin, il devra être en mesure de fournir des rapports réguliers sur l'état d'avancement des campagnes et sur les résultats obtenus ;
* Taux de réussite des campagnes de test de phishing et vishing, mesuré par le nombre de personnes qui ont succombé aux tentatives d'hameçonnage et le nombre total de personnes testées ;
* Taux de réussite des campagnes de social engineering, mesuré par le nombre de personnes qui ont succombé aux tentatives de manipulation et le nombre total de personnes testées ;
* Nombre de participants aux sessions de formation aux risques de phishing, vishing et social engineering ;
* Niveau de satisfaction des participants aux sessions de formation, mesuré par un questionnaire de satisfaction ;
* Taux de mise en place des mesures de prévention recommandées pour donner suite à la campagne de formation (par exemple, utilisation de mots de passe forts, activation de la double authentification, etc.).

## Lot A4 - Cyber Threat Intelligence

## Objectifs du lot

Le lot de "Cyber Threat Intelligence" vise à fournir aux Pouvoirs locaux wallons une vision globale et à jour des menaces cybers auxquelles ils sont exposés. Ce service comprend la collecte, l'analyse et la diffusion d'informations sur les menaces actuelles et émergentes, ainsi que des recommandations pour les contrer.

L’attributaire doit :

* Fournir une vision globale et à jour des menaces cybernétiques auxquelles les Pouvoirs locaux wallons sont exposés ;
* Contribuer à améliorer la préparation et la résilience face aux incidents de cybersécurité ;
* Faciliter la prise de décisions en matière de sécurité en fournissant une intelligence stratégique et opérationnelle ;
* Collecter et analyser des données sur les menaces et les campagnes de cybersécurité en cours afin de fournir des informations sur les menaces potentielles et les tendances émergentes;
* Identifier les acteurs malveillants et leurs techniques, méthodes et outils pour aider à la prévention et à la détection des attaques;
* Fournir des alertes et des mises à jour sur les menaces spécifiques et les campagnes ciblant les Pouvoirs locaux wallons;
* Fournir des conseils et des recommandations pour renforcer la sécurité en fonction des menaces identifiées;
* Intégrer des informations de menace avec les systèmes de sécurité existants pour une meilleure prévention et détection des attaques.

## Caractéristiques spécifiques du lot

Les caractéristiques spécifiques de ce lot de Cyber Threat Intelligence visent à garantir que les Pouvoirs locaux wallons disposent des outils et des fonctionnalités nécessaires pour protéger efficacement leurs systèmes et leurs données contre les menaces cybernétiques. Ces caractéristiques comprendront notamment :

* Mise en place d'un système de détection des intrusions pour détecter les attaques à un stade précoce ;
* Mise en place d'un système d'analyse des données de menace pour identifier les tendances et les campagnes d'attaque en cours ;
* Mise en place d'un système de gestion des alertes pour informer rapidement les Pouvoirs locaux de toute menace détectée ;
* Mise en place d'un système de gestion des incidents pour permettre une réponse rapide et efficace aux attaques ;
* Intégration avec les systèmes de sécurité existants des Pouvoirs locaux pour une protection renforcée ;
* Fourniture d'un portail web pour accéder aux données de menace et aux alertes en temps réel ;
* Fourniture de rapports réguliers sur les menaces détectées et les actions prises pour les contrer.

## Spécificités techniques

Les spécificités techniques de ce lot de Cyber Threat Intelligence visent à garantir que les outils et les fonctionnalités proposés répondent aux exigences en matière de sécurité et de performance pour les Pouvoirs locaux wallons. Ces spécificités comprendront notamment :

* Mise en place d'une architecture de sécurité distribuée pour assurer une protection renforcée des systèmes et des données des Pouvoirs locaux ;
* Utilisation de technologies de dernière génération pour détecter les menaces cybers ;
* Mise en place d'une architecture de sécurité adaptable pour s'adapter aux évolutions des menaces cybers ;
* Utilisation de protocoles de sécurité standard pour protéger les communications ;
* Utilisation de la cryptographie pour protéger les données sensibles ;
* Mise en place de systèmes de sauvegarde pour protéger les données en cas de pannes
* Mise en place d'un système de suivi des acteurs malveillants pour identifier les groupes et les individus responsables des attaques ;
* Mise en place d'un système de veille des réglementations et des normes pour assurer la conformité aux exigences en matière de sécurité ;
* Mise en place d'un système de veille des tendances technologiques pour identifier les nouvelles technologies de sécurité et les intégrer aux systèmes des Pouvoirs locaux ;
* Mise en place d'un système de veille des incidents pour identifier les tendances des attaques et les modèles d'attaque ;
* Mise en place d'un système de veille des vulnérabilités pour identifier les faiblesses dans les systèmes et les réseaux des Pouvoirs locaux ;
* Mise en place d'un système de veille des menaces sur les réseaux sociaux pour identifier les campagnes de phishing et les attaques ciblées ;
* Mise en place d'un système de veille des menaces sur le dark web pour identifier les outils et les techniques utilisés par les cybercriminels ;
* Mise en place d'un système de veille des menaces sur les forums et les blogs pour identifier les informations et les techniques utilisées par les cybercriminels ;
* Mise en place d'un système de veille des menaces sur les téléphones et les tablettes pour identifier les menaces sur ces plateformes.

## Domaines d’expertise

Pour répondre spécifiquement à ce lot de Cyber Threat Intelligence, il est recommandé de demander aux soumissionnaires les domaines d'expertise suivants:

* Analyse de menaces: Connaissance des différentes méthodes d'analyse des menaces et des techniques utilisées pour identifier les attaques ;
* Intelligence artificielle et analyse de données: Connaissance de l'utilisation de l'intelligence artificielle et de l'analyse de données pour détecter les menaces et identifier les tendances ;
* Cryptographie: Connaissance des différents algorithmes de chiffrement et des protocoles de sécurité pour protéger les données ;
* Réglementation et conformité: Connaissance des normes et des réglementations en matière de sécurité de l'information et de la cybersécurité ;
* Ingénierie de sécurité: Connaissance des techniques d'ingénierie de sécurité pour identifier les vulnérabilités et les faiblesses dans les systèmes et les réseaux ;
* Veille des menaces: Connaissance des techniques et des outils pour surveiller les menaces en temps réel et identifier les tendances ;
* Anonymisation des données: Connaissance des techniques pour protéger les données des utilisateurs et respecter leur vie privée ;
* Connaissance de la réglementation en matière de données: Connaissance de la réglementation en matière de protection des données et de respect des normes en vigueur comme le RGPD ;
* Connaissance des systèmes de détection d'intrusion (IDS) et de prévention d'intrusion (IPS) pour protéger les systèmes et les réseaux ;
* Connaissance des systèmes de gestion de la sécurité (SMS) pour gérer les systèmes et les réseaux de manière sécurisée ;
* Connaissance des systèmes de chiffrement pour protéger les données sensibles ;
* Connaissance des systèmes de gestion des vulnérabilités pour identifier les faiblesses dans les systèmes et les réseaux ;
* Connaissance des systèmes de détection de la compromission de l'identité pour identifier les comptes compromis ;
* Connaissance des systèmes de gestion des configurations pour garantir la conformité aux normes de sécurité ;
* Connaissance des systèmes de gestion des patches pour maintenir les systèmes à jour et corriger les vulnérabilités ;
* Connaissance des systèmes de gestion des logs pour suivre les activités sur les systèmes et les réseaux ;
* Connaissance des normes et des référentiels en matière de cybersécurité tels que ISO 27001, NIST, etc.

## Rapports et documentations

Pour répondre à ce lot de Cyber Threat Intelligence, l’attributaire devra fournir les documents et rapports suivants :

* Un plan de gestion des menaces détaillant les processus et les outils utilisés pour surveiller les menaces et répondre aux attaques ;
* Des cahiers des charges pour les systèmes et les outils proposés, décrivant les fonctionnalités et les exigences techniques ;
* Des spécifications détaillées pour les systèmes et les outils proposés, décrivant les exigences en matière de performance, de disponibilité et de scalabilité ;
* Des scénarios d'utilisation pour les systèmes et les outils proposés, décrivant comment ils seront utilisés pour protéger les Pouvoirs locaux contre les menaces cybers ;
* Des études de cas et des références clients pour les systèmes et les outils proposés, décrivant les résultats ;
* Des documents de conformité aux normes et aux réglementations en vigueur, tels que les certifications ISO 27001 ou SOC 2 ;
* Des documents de garantie pour les systèmes et les outils proposés ;
* Des documents de maintenance pour les systèmes et les outils proposés ;
* Des documents de support pour les systèmes et les outils proposés.

## Obligation de résultat

Pour répondre spécifiquement à ce lot de Cyber Threat Intelligence, il est attendu des soumissionnaires les obligations de résultats suivantes :

* Mise en place d'un système de veille de la cybersécurité pour identifier les nouvelles menaces et les vulnérabilités ;
* Mise en place d'un système de suivi des acteurs malveillants pour identifier les groupes et les individus responsables des attaques ;
* Mise en place d'un système de veille des menaces sur le dark web pour identifier les outils et les techniques utilisés par les cybercriminels ;
* Mise en place d'un système de veille des menaces sur les forums et les blogs pour identifier les informations et les techniques utilisées par les cybercriminels ;
* Mettre en place un système de notification en temps réel pour alerter les Pouvoirs locaux des menaces identifiées.

## Lot A5 - Accompagnement DPD/DPO à la demande

Pour s'assurer d'une expertise adéquate pour ce lot de DPO à la demande, les soumissionnaires doivent avoir des connaissances et des compétences dans les domaines suivants :

* Connaissance approfondie des réglementations en matière de protection des données personnelles, notamment le RGPD ;
* Expérience pratique en matière de mise en œuvre de politiques et de procédures de protection des données ;
* Connaissance des méthodes et outils de gestion des incidents de protection des données ;
* Compétences en matière de sensibilisation et de formation du personnel sur les bonnes pratiques en matière de protection des données ;
* Connaissance des techniques de sécurité des données telles que le chiffrement, la gestion des accès, la sauvegarde des données, etc. ;
* Expérience en matière de traitement de demandes d'exercice des droits des personnes concernées et de gestion des notifications d'incident de protection des données ;
* Connaissance des normes nationales et internationales de sécurité ;
* Compétence en matière de mise en œuvre de politiques, procédures et processus de sécurité de l'information.

## Objectifs du lot

Le lot "DPO à la demande" a pour objectif de fournir aux Pouvoirs locaux wallons une solution flexible et sur mesure pour gérer leur protection des données personnelles. Ce service de DPD/DPO (Délégué à la Protection des Données) à la demande permettra aux Pouvoirs locaux de se conformer aux exigences réglementaires en matière de protection des données, tout en préservant la continuité de leurs missions et la sécurité des informations sensibles de leurs citoyens.

Objectifs:

* Fournir une solution flexible et adaptée aux besoins spécifiques des Pouvoirs locaux wallons en matière de protection des données personnelles ;
* Assurer la conformité aux exigences réglementaires en matière de protection des données ;
* Garantir la continuité de service des missions des Pouvoirs locaux ;
* Protéger les informations sensibles des citoyens des Pouvoirs locaux ;
* Offrir un soutien expert en matière de protection des données pour les Pouvoirs locaux wallons ;
* Fournir une assistance pour la mise en place de politiques et de procédures de protection des données ;
* Sensibiliser les employés des Pouvoirs locaux à la nécessité de la protection des données personnelles ;
* Aider les Pouvoirs locaux à gérer les demandes de protection des données de leurs citoyens et les obligations de notification en cas de violation de données ;
* Offrir un suivi régulier et une évaluation continue des pratiques de protection des données pour les Pouvoirs locaux.

## Caractéristiques spécifiques du lot

Pour garantir que les services proposés répondent aux besoins spécifiques de notre organisation, nous attendons des soumissionnaires qu'ils démontrent des caractéristiques spécifiques liées à fourniture d’un DPD/DPO à la demande. Les soumissionnaires doivent décrire comment ils comptent mettre en œuvre ces caractéristiques pour répondre aux besoins de notre projet :

* Services de protection des données personnelles pour les Pouvoirs locaux ;
* Personnel qualifié et expert en matière de protection des données personnelles ;
* Critères de sélection rigoureux pour les prestataires de services ;
* Engagement en faveur de la protection des données personnelles des citoyens ;
* Mécanismes de suivi et de mesure de la qualité des services fournis ;
* Formation continue pour les employés des Pouvoirs locaux sur les questions de protection des données personnelles ;
* Compétence en matière de protection des données personnelles ;
* Connaissance approfondie des réglementations européennes en matière de protection des données personnelles, telles que le RGPD ;
* Expérience en matière de mise en œuvre de politiques de protection des données et de mise en conformité avec les réglementations applicables ;
* Capacité à établir des relations de confiance avec les employés et les différentes parties prenantes ;
* Compréhension approfondie des processus de traitement des données et des mécanismes de protection des données personnelles ;
* Expérience en matière de gestion des incidents de protection des données et de résolution de conflits liés à la protection des données.

## Réglementations en vigueur

En plus de la politique interne, et des directives IT en matière de matériel et de logiciel, les soumissionnaires sélectionnés devront adhérer à toutes les lois applicables du pays et aux règles, réglementations et directives prescrites par les différentes autorités réglementaires, statutaires et gouvernementales:

* Le Règlement Général de la Protection des Données ;
* Directives CCB ;
* Dernière version de la norme ISO27001 ;
* La directive NIS2

iMio se réserve le droit de vérifier les informations auprès des autres sociétés et institutions auxquelles les soumissionnaires ont fourni leurs services pour l'exécution de projets similaires.

## Domaines d’expertise

Pour s'assurer d'une expertise adéquate pour ce lot de DPO à la demande, les soumissionnaires peuvent être demandés d'avoir des connaissances et des compétences dans les domaines suivants :

* Connaissance approfondie des règlementations en matière de protection des données personnelles, notamment le RGPD ;
* Expérience pratique en matière de mise en œuvre de politiques et de procédures de protection des données ;
* Connaissance des méthodes et outils de gestion des incidents de protection des données ;
* Compétences en matière de sensibilisation et de formation du personnel sur les bonnes pratiques en matière de protection des données ;
* Connaissance des techniques de sécurité des données telles que le chiffrement, la gestion des accès, la sauvegarde des données, etc. ;
* Expérience en matière de traitement de demandes d'exercice des droits des personnes concernées et de gestion des notifications d'incident de protection des données ;
* Connaissance des normes nationales et internationales de sécurité.

Compétence en matière de mise en œuvre de politiques, procédures et processus de sécurité de l'information.

## Rapports et documentations

Pour nous permettre d'évaluer la qualité de travail des soumissionnaires, nous attendons qu'ils fournissent des rapports et des documentations détaillés sur l'exercice de leur fonction en tant que DPD à la demande. Les soumissionnaires doivent décrire les types de rapports et de documentations qu'ils comptent fournir pour répondre aux besoins de notre projet :

* Présentation détaillée des méthodologies et des processus de travail utilisés ;
* Des échantillons de rapports précédents sur des projets similaires ;
* Des exemples concrets d'actions menées pour améliorer la protection de la vie privée des personnes concernées ;
* Une description détaillée des outils et technologies utilisées pour garantir la conformité avec les réglementations applicables en matière de protection de la vie privée ;
* Des informations sur les formations et certifications obtenues par le personnel en charge du projet ;
* Certificats et accréditations en matière de protection de données et de confidentialité ;
* Historique de mise en œuvre de solutions de protection de la vie privée pour des clients similaires ;
* Preuve de la conformité aux réglementations et aux normes industrielles en matière de protection de données ;
* Exemples de cas réussis de gestion des incidents de sécurité ;
* Évaluations régulières de la sécurité de l'information par un tiers indépendant.

## Obligation de résultat

Afin d'assurer l'efficacité du service de DPD/DPO à la demande, il est crucial de définir clairement les obligations de résultats attendues des soumissionnaires. Les éléments suivants doivent être pris en compte lors de l'établissement de ces obligations :

* Obligation de mener des audits réguliers pour identifier les risques potentiels pour la protection des données ;
* Engagement de respecter les lois et réglementations en matière de protection des données, telles que le RGPD ;
* Mise en place de mesures de sécurité techniques et organisationnelles pour protéger les données sensibles
* Fourniture de rapports réguliers sur les activités liées à la protection des données pour assurer un suivi adéquat et une transparence. ;
* La formation des employés pour garantir la compréhension et la conformité aux politiques de protection des données ;
* La mise à disposition de ressources pour gérer les incidents de protection des données et les violations de sécurité ;
* La participation à des programmes d'évaluation de la conformité pour vérifier la qualité du système de gestion de la protection des données ;

L’organisation de formation pour les agents des pouvoir locaux afin de démystifier le RGPD et de les former aux données personnelles.

## Lot A6 - RSSI as a service

Pour s'assurer d'une expertise adéquate, les soumissionnaires doivent avoir des connaissances et des compétences dans les domaines suivants :

* Capacité à réaliser des évaluations de risques de sécurité et à fournir des plans d'actions détaillés pour les atténuer ;
* Capacité à élaborer et à fournir des formations et des sensibilisations en matière de sécurité de l'information aux employés des Pouvoirs locaux wallons ;
* Connaissance des pratiques et des technologies émergentes en matière de sécurité de l'information ;
* Expérience en gestion de la sécurité de l'information dans des environnements complexes et/ou réglementés ;
* Connaissance des normes et des bonnes pratiques en matière de sécurité de l'information, telles que ISO 27001 ou CIS Critical Security Controls ;
* Connaissance des réglementations en matière de protection des données, telles que le RGPD et la directive NIS ;
* Capacité à analyser les risques de sécurité de l'information et à recommander des mesures d'atténuation appropriées ;
* Expérience en matière de gestion d'incidents de sécurité de l'information, y compris la préparation, la réponse et la récupération ;
* Connaissance des technologies de sécurité de l'information, telles que les pare-feu, les antivirus, les IDS/IPS, la gestion des identités et des accès, etc. ;
* Connaissance des méthodologies d'évaluation de la sécurité de l'information, telles que les tests de pénétration, les tests de vulnérabilité et les évaluations de la conformité ;
* Capacité à élaborer et à mettre en œuvre des politiques, des procédures et des plans de sécurité de l'information

## Objectifs du lot

La sécurité de l'information est devenue un enjeu majeur pour les organisations publiques et privées. Pour les Pouvoirs locaux wallons, il est primordial de protéger les données sensibles de leurs citoyens et de garantir la continuité de leurs services en cas d'incident. Le lot RSSI/CISO à la demande a pour objectif de fournir des services de conseil et d'expertise en sécurité de l'information pour accompagner les Pouvoirs locaux wallons dans la gestion de leur sécurité.

Objectifs:

* Fournir un service de conseil et d'expertise en sécurité de l'information aux Pouvoirs locaux wallons ;
* Accompagner les Pouvoirs locaux wallons dans la définition de leur politique de sécurité de l'information ;
* Identifier et évaluer les risques de sécurité de l'information auxquels sont exposés les Pouvoirs locaux wallons ;
* Proposer des mesures de sécurité adaptées aux besoins et contraintes des Pouvoirs locaux wallons ;
* Conseiller les Pouvoirs locaux wallons dans la mise en place et l'amélioration de leurs dispositifs de sécurité de l'information ;
* Assurer une veille réglementaire et technologique pour garantir la conformité et l'efficacité des mesures de sécurité mises en place par les Pouvoirs locaux wallons.

## Caractéristiques spécifiques du lot

Le lot de RSSI/CISO à la demande a pour objectif de fournir aux Pouvoirs locaux wallons un service de sécurité informatique de haute qualité en mettant à disposition des experts de la sécurité de l'information pour répondre à leurs besoins.

En voici les caractéristiques spécifiques :

* La fourniture d'un CISO/RSSI sur demande, permettant une gestion et une coordination de la sécurité des systèmes d'information ;
* L'analyse et l'évaluation des risques liés aux données sensibles des Pouvoirs locaux wallons
* La mise en place de plans de gestion des incidents en cas de cyber-attaques et la prise en charge des actions correctives nécessaires
* La réalisation d'audits de sécurité réguliers pour assurer la conformité des systèmes d'information des Pouvoirs locaux wallons aux normes et standards en vigueur
* L'accompagnement des Pouvoirs locaux wallons dans la mise en œuvre de politiques de sécurité de l'information et de formation des utilisateurs.

## Réglementations en vigueur

En plus de la politique interne, et des directives IT en matière de matériel et de logiciel, les soumissionnaires sélectionnés devront adhérer à toutes les lois applicables du pays et aux règles, réglementations et directives prescrites par les différentes autorités réglementaires, statutaires et gouvernementales :

* Le Règlement Général de la Protection des Données ;
* Directives CCB ;
* Dernière version de la norme ISO27001 ;
* La directive NIS2

iMio se réserve le droit de vérifier les informations auprès des autres sociétés et institutions auxquelles les soumissionnaires ont fourni leurs services pour l'exécution de projets similaires.

## Domaines d’expertises

Pour s'assurer d'une expertise adéquate, les soumissionnaires peuvent être demandés d'avoir des connaissances et des compétences dans les domaines suivants :

* Capacité à réaliser des évaluations de risques de sécurité et à fournir des plans d'actions détaillés pour les atténuer ;
* Capacité à élaborer et à fournir des formations et des sensibilisations en matière de sécurité de l'information aux employés des Pouvoirs locaux wallons ;
* Connaissance des pratiques et des technologies émergentes en matière de sécurité de l'information ;
* Expérience en gestion de la sécurité de l'information dans des environnements complexes et/ou réglementés ;
* Connaissance des normes et des bonnes pratiques en matière de sécurité de l'information, telles que ISO 27001 ou CIS Critical Security Controls ;
* Connaissance des réglementations en matière de protection des données, telles que le RGPD et la directive NIS ;
* Capacité à analyser les risques de sécurité de l'information et à recommander des mesures d'atténuation appropriées ;
* Expérience en matière de gestion d'incidents de sécurité de l'information, y compris la préparation, la réponse et la récupération ;
* Connaissance des technologies de sécurité de l'information, telles que les pare-feu, les antivirus, les IDS/IPS, la gestion des identités et des accès, etc. ;
* Connaissance des méthodologies d'évaluation de la sécurité de l'information, telles que les tests de pénétration, les tests de vulnérabilité et les évaluations de la conformité ;
* Capacité à élaborer et à mettre en œuvre des politiques, des procédures et des plans de sécurité de l'information.

## Rapports et documentations

Pour garantir la qualité du service, nous demandons aux soumissionnaires de fournir les documents et rapports suivants :

* Un plan de gestion de la sécurité de l'information (PGSI) qui décrit les mesures de sécurité mises en place pour protéger les données et les systèmes ;
* Un rapport d'audit de sécurité récent, réalisé par une tierce partie indépendante, qui démontre que les mesures de sécurité décrites dans le PGSI sont effectivement mises en place et efficaces ;
* Les certifications de sécurité pertinentes, telles que CISSP, CISM, CISA, CEH, etc.
* Des références clients pour des missions similaires, y compris des informations sur la portée de la mission, les résultats obtenus, la qualité du service et la satisfaction du client ;
* Des informations sur leur méthodologie d'évaluation des risques et de gestion de la sécurité, ainsi que sur les outils qu'ils utilisent pour effectuer ces tâches ;
* Des informations sur leurs politiques de confidentialité et de sécurité de l'information, y compris la gestion des données personnelles et des données sensibles ;
* Des informations sur leur capacité à fournir des services de conseil en sécurité, y compris leur expérience en matière d'audit de sécurité, de tests d'intrusion et de formation en sécurité.

Ces documents permettront d'évaluer la capacité des soumissionnaires à fournir un service de qualité en matière de sécurité de l'information.

## Obligation de résultat

Afin d'assurer l'efficacité du service de RSSI/CISO à la demande, il est crucial de définir les obligations de résultats attendues des soumissionnaires. Les éléments suivants doivent être pris en compte lors de l'établissement de ces obligations :

* Élaboration et mise en œuvre d'un plan de sécurité adapté aux besoins de l'organisation ;
* Surveillance régulière de la sécurité des systèmes d'information et mise en place de mesures correctives en cas de violation ou de faille de sécurité ;
* Réalisation d'audits de sécurité réguliers ;
* Assistance en cas d'incidents de sécurité tels que des attaques informatiques ou des violations de données;
* Respect des normes de sécurité et des exigences légales et réglementaires ;applicables en matière de sécurité des systèmes d'information ;
* Fourniture de rapports réguliers sur l'état de la sécurité des systèmes d'information et les mesures prises pour l'améliorer ;
* Respecter les normes de sécurité en vigueur (ISO 27001, RGPD, etc.) ;
* Assurer une surveillance continue de la sécurité de l'organisation pour détecter les menaces et les incidents de sécurité le plus tôt possible ;
* Établir des plans d'actions pour résoudre les problèmes de sécurité identifiés et les mettre en œuvre dans les délais impartis.

1. **FORMULAIRE D'OFFRE**

OFFRE DE PRIX POUR LE MARCHE AYANT POUR OBJET  
“ CENTRALE D'ACHAT POUR PRESTATIONS D’ACCOMPAGNEMENT EN MATIÈRE DE CYBERSÉCURITÉ ”

Procédure ouverte

*Important : ce formulaire doit être complété dans son entièreté.*

Personne physique  
Le soussigné (nom et prénom) :  
Qualité ou profession :  
Nationalité :  
Domicile (adresse complète) :

Téléphone :  
GSM :  
Fax :  
E-mail :  
Personne de contact :

**Soit (1)**

Personne morale  
La firme (dénomination, raison sociale) :  
Nationalité :  
ayant son siège à (adresse complète) :

Téléphone :  
GSM :  
Fax :  
E-mail :  
Personne de contact :

représentée par le(s) soussigné(s) :  
(Les mandataires joignent à leur offre l'acte authentique ou sous seing privé qui leur accorde ses pouvoirs ou une copie de la procuration. Ils peuvent se borner à indiquer le numéro de l'annexe du Moniteur belge qui a publié l'extrait de l'acte concerné.)

**Soit (1)**

Groupement d'opérateurs économiques (y compris la société simple)  
  
Nom et prénom ou raison sociale des soumissionnaires et forme juridique :

Qualité ou profession :

Nationalité :

Adresse ou siège social :

Téléphone :

GSM :

E-mail :

Personne de contact :

Nom et prénom ou raison sociale des soumissionnaires et forme juridique :

Qualité ou profession :

Nationalité :

Adresse ou siège social :

Téléphone :

GSM :

E-mail :

Personne de contact :

Ces données doivent être complétées pour chacun des participants au groupement.

Le groupement est représenté par l'un des participants, dont le nom est :

S'ENGAGE(NT) À EXÉCUTER LE MARCHÉ CONFORMÉMENT AUX CLAUSES ET CONDITIONS DU CAHIER DES CHARGES DU MARCHÉ PUBLIC SUSMENTIONNÉ (PO/001/2023/ACC) :

**Lot A1 : Rédaction et accompagnement à la mise en œuvre des politiques de sécurité**

pour un montant de :

(en chiffres, TVA comprise)

…................................................................................................................................................

(en lettres, TVA comprise)

…................................................................................................................................................

…................................................................................................................................................

**Lot A2 : Évaluation des vulnérabilités et « Pen-tests »**

pour un montant de :

(en chiffres, TVA comprise)

…................................................................................................................................................

(en lettres, TVA comprise)

…................................................................................................................................................

…................................................................................................................................................

**Lot A3 : Campagne de test de phishing/vishing/social engineering**

pour un montant de :

(en chiffres, TVA comprise)

…................................................................................................................................................

(en lettres, TVA comprise)

…................................................................................................................................................

…................................................................................................................................................

**Lot A4 : Cyber threat intelligence**

pour un montant de :

(en chiffres, TVA comprise)

…................................................................................................................................................

(en lettres, TVA comprise)

…................................................................................................................................................

…................................................................................................................................................

**Lot A5 : Accompagnement dpd/dpo à la demande**

pour un montant de :

(en chiffres, TVA comprise)

…................................................................................................................................................

(en lettres, TVA comprise)

…................................................................................................................................................

…................................................................................................................................................

**Lot A6 : RSSI as a service**

pour un montant de :

(en chiffres, TVA comprise)

…................................................................................................................................................

(en lettres, TVA comprise)

…................................................................................................................................................

…................................................................................................................................................

Informations générales

Numéro d'immatriculation à l'ONSS :  
Numéro d'entreprise (en Belgique uniquement) :  
Le soumissionnaire est une micro-, petite ou moyenne entreprise : OUI / NON *(biffer les mentions inutiles)* **(2)**

Sous-traitants

Il sera fait appel à des sous-traitants : OUI / NON *(biffer les mentions inutiles)*

Part du marché sous-traitée :

Il sera fait appel aux sous-traitants suivants :

Personnel

Du personnel soumis à la législation sociale d'un autre pays membre de l'Union européenne est employé :

OUI / NON *(biffer les mentions inutiles)*

Cela concerne le pays membre de l'UE suivant :

Paiements

Les paiements seront effectués valablement par virement ou versement sur le compte (IBAN/BIC) ................................................ de l'institution financière ................................. ouvert au nom de ................................. .

Attestations

A cette offre je joins/nous joignons :  
\* Le DUME, par lequel l'opérateur économique déclare qu’il ne se trouve pas dans une des situations d’exclusion visées aux articles 67 à 69 de la loi du 17 juin 2016.

Documents à joindre à l'offre

À cette offre, sont également joints :

- les documents que le cahier des charges impose de fournir ;

- les modèles, échantillons et autres informations, que le cahier des charges impose de fournir.

À savoir :

* Le(s) DUME(s)
* Annexe A : le formulaire d’offre
* Annexe B : Inventaire (s)
* Annexe C : Bordereau(x) de réponse technique
* Annexe G : Engagements sur l’Obligation de résultats
* Un document récapitulatif de l’offre de service proposée ainsi qu’une présentation de la société ;
* Les curriculums vitae des personnes les identifiant de manière unique (Cfr liste expert annexe C)
* Les fiches produits/logiciels des fabricants/éditeurs proposés
* Toute(s) autre(s) annexe(s) nécessaire(s) à la bonne complétion du dossier

Fait à ...........................................................................................................................................

Le ................................................................................................................................................

Le soumissionnaire,

Nom et prénom : ..........................................................................................................................

Fonction : .....................................................................................................................................

Note importante

Les soumissionnaires ne peuvent se prévaloir des vices de forme dont est entachée leur offre, ni des erreurs ou omissions qu'elle comporte (article 82 de l'arrêté royal du 18 avril 2017).

**(1) Biffer les mentions inutiles**

**(2)** Au sens de la recommandation de la Commission Européenne du 6 mai 2013 concernant la définition des micro-, petites et moyennes entreprises.

Microentreprise : Entreprise qui occupe moins de 10 personnes et dont le chiffre d'affaire annuel ou le total du bilan annuel n'excède pas 2 millions d'euros.

Petite entreprise : Entreprise qui occupe moins de 50 personnes et dont le chiffre d'affaire annuel ou le total du bilan annuel n'excède pas 10 millions d'euros.

Moyenne entreprise : Entreprise qui n'est ni une micro- ni une petite entreprise et qui occupe moins de 250 personnes et dont le chiffre d'affaire annuel n'excède pas 50 millions d'euros et/ou le total du bilan annuel ne dépasse pas 43 millions d'euros.

1. **INVENTAIRE**

OFFRE DE PRIX POUR LE MARCHÉ AYANT POUR OBJET

“ CENTRALE D'ACHAT POUR PRESTATIONS D’ACCOMPAGNEMENT EN MATIÈRE DE CYBERSÉCURITÉ ”

“LOT A1 : Rédaction et accompagnement des politiques de sécurité”

| **N°** | **Description** | **Taille PL** | **Type** | **Unité** | **Q** | **PU en chiffres HTVA** | **Total HTVA** | **%TVA** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Mise en place d'un processus de rédaction de politiques de sécurité adapté aux besoins des Pouvoirs locaux wallons et conforme aux réglementations en vigueur pour un Pouvoir local[[2]](#footnote-1) | <50 employés | QP | Forfait | 88 | € | € | % |
| 50 à 100 employés | QP | Forfait | 57 | € | € | % |
| 100 à 500 employés | QP | Forfait | 46 | € | € | % |
| > 500 employés | QP | Forfait | 10 | € | € | % |
| 2 | Coordinateur de projet | N/A | QP | Jour-homme | 50 | € | € | % |
| 3 | Expert Senior | N/A | QP | Jour-homme | 200 | € | € | % |
| 4 | Expert Junior | N/A | QP | Jour-homme | 100 | € | € | % |

| **Total HTVA :** |  |
| --- | --- |
| **TVA :** |  |
| **Total TVAC :** |  |

| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| --- |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à .......................................... le ...................................................... Fonction : ......................................................  Nom et prénom : .................................................................... |

OFFRE DE PRIX POUR LE MARCHÉ AYANT POUR OBJET

“ CENTRALE D'ACHAT POUR PRESTATIONS D’ACCOMPAGNEMENT EN MATIÈRE DE CYBERSÉCURITÉ ”

“ Lot A2 : Évaluation des vulnérabilités et pen tests”

| **N°** | **Description** | **Type** | **Unité** | **Q** | **PU en chiffres HTVA** | **Total HTVA** | **%TVA** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Coordinateur de projet | QP | Jour-homme | 50 | € | € | % |
| 2 | Expert Senior | QP | Jour-homme | 200 | € | € | % |
| 3 | Expert Junior | QP | Jour-homme | 100 | € | € | % |
| 4 | Logiciel/service utilisé | QP | Licence[[3]](#footnote-2) | 176 | € | € | % |

| **Total HTVA :** |  |
| --- | --- |
| **TVA :** |  |
| **Total TVAC :** |  |

| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| --- |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à .......................................... le ...................................................... Fonction : ......................................................  Nom et prénom : .................................................................... |

OFFRE DE PRIX POUR LE MARCHÉ AYANT POUR OBJET

“ CENTRALE D'ACHAT POUR PRESTATIONS D’ACCOMPAGNEMENT EN MATIÈRE DE CYBERSÉCURITÉ ”

“Lot A3 : Campagne de test de phishing/vishing/social engineering”

| **N°** | **Description** | **Type** | **Unité** | **Q** | **PU en chiffres HTVA** | **Total HTVA** | **%TVA** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Coordinateur de projet | QP | Jour-homme | 50 | € | € | % |
| 2 | Expert Senior | QP | Jour-homme | 200 | € | € | % |
| 3 | Expert Junior | QP | Jour-homme | 100 | € | € | % |
| 4 | Logiciel/service utilisé | QP | licence[[4]](#footnote-3) | 18414 | € | € | % |

| **Total HTVA :** |  |
| --- | --- |
| **TVA :** |  |
| **Total TVAC :** |  |

| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| --- |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à .......................................... le ...................................................... Fonction : ......................................................  Nom et prénom : .................................................................... |

OFFRE DE PRIX POUR LE MARCHÉ AYANT POUR OBJET

“ CENTRALE D'ACHAT POUR PRESTATIONS D’ACCOMPAGNEMENT EN MATIÈRE DE CYBERSÉCURITÉ ”

“Lot A4: Cyber Threat Intelligence”

| **N°** | **Description** | **Type** | **Unité** | **Q** | **PU en chiffres HTVA** | **Total HTVA** | **%TVA** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Coordinateur de projet | QP | Jour-homme | 50 | € | € | % |
| 2 | Expert Senior | QP | Jour-homme | 200 | € | € | % |
| 3 | Expert Junior | QP | Jour-homme | 100 | € | € | % |
| 4 | Logiciel/service utilisé | QP | Licence[[5]](#footnote-4) | 208 | € | € | % |

| **Total HTVA :** |  |
| --- | --- |
| **TVA :** |  |
| **Total TVAC :** |  |

| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| --- |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à .......................................... le ...................................................... Fonction : ......................................................  Nom et prénom : .................................................................... |

OFFRE DE PRIX POUR LE MARCHÉ AYANT POUR OBJET

“ CENTRALE D'ACHAT POUR PRESTATIONS D’ACCOMPAGNEMENT EN MATIÈRE DE CYBERSÉCURITÉ ”

“Lot A5: Accompagnement DPD/DPO à la demande”

| **N°** | **Description** | **Type** | **Unité** | **Q** | **PU en chiffres HTVA** | **Total HTVA** | **%TVA** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Coordinateur de projet | QP | Jour-homme | 50 | € | € | % |
| 2 | Expert Senior | QP | Jour-homme | 200 | € | € | % |
| 3 | Expert Junior | QP | Jour-homme | 100 | € | € | % |
|  |  |  |  |  |  |  |  |

| **Total HTVA :** |  |
| --- | --- |
| **TVA :** |  |
| **Total TVAC :** |  |

| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| --- |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à .......................................... le ...................................................... Fonction : ......................................................  Nom et prénom : .................................................................... |

OFFRE DE PRIX POUR LE MARCHE AYANT POUR OBJET

“ CENTRALE D'ACHAT POUR PRESTATIONS D’ACCOMPAGNEMENT EN MATIÈRE DE CYBERSÉCURITÉ ”

“Lot A6: RSSI as a service”

| **N°** | **Description** | **Type** | **Unité** | **Q** | **PU en chiffres HTVA** | **Total HTVA** | **%TVA** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Coordinateur de projet | QP | Jour-homme | 50 | € | € | % |
| 2 | Expert Senior | QP | Jour-homme | 200 | € | € | % |
| 3 | Expert Junior | QP | Jour-homme | 100 | € | € | % |
|  |  |  |  |  |  |  |  |

| **Total HTVA :** |  |
| --- | --- |
| **TVA :** |  |
| **Total TVAC :** |  |

| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| --- |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à .......................................... le ...................................................... Fonction : ......................................................  Nom et prénom : .................................................................... |

1. **BORDEREAU DE RÉPONSE TECHNIQUE**

OFFRE DE PRIX POUR LE MARCHE AYANT POUR OBJET  
“ CENTRALE D'ACHAT POUR PRESTATIONS D’ACCOMPAGNEMENT EN MATIÈRE DE CYBERSÉCURITÉ ”

Procédure ouverte

Les tableaux présentés ci-dessous sont téléchargeables via le lien suivant : https://docs.google.com/spreadsheets/d/1IiqbqCX9zmKwgHTtJQtZVWLhW2eWL-mSD9LRtqozIdc/edit?usp=sharing

Lot A1 - Rédaction et accompagnement des politiques de sécurité

**Critère d’attribution 2.1 - Maîtrise des domaines d’expertise**

Le niveau d’expertise attendu des experts est décrit ci-après selon une catégorisation des domaines d'expertise. Une profil qui n’atteint pas 75% des compétences attendues sera déclaré irrégulier, ceci entraînant son exclusion du marché, si le profil exclu rend le nombre d’experts insuffisant au regard des critères de sélection qualitative, l’offre du soumissionnaire sera écartée, pour le lot concerné.

Le curriculum vitae soumis doit attester de la maîtrise des domaines revendiqués. Dans ce tableau, utilisé pour évaluer le 2ème critère d’attribution, le soumissionnaire indique dans chaque compétence marquée comme détenue l’expérience professionnelle du CV relative à ce domaine d’expertise.

| **#** | **Domaines d'expertise** | **Expert 1 - N° de CV** | **Expert 2 - N° de CV** | **Expert 3 - N° de CV** |
| --- | --- | --- | --- | --- |
| 1 | Connaissance des réglementations et normes en matière de sécurité de l'information, telles que ISO 27001 et GDPR ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 2 | Expérience de la rédaction de politiques de sécurité pour les organisations publiques et/ou de grande taille ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 3 | Connaissance des meilleures pratiques en matière de gestion de la sécurité de l'information, y compris la mise en place de contrôles de sécurité, la gestion des risques et la gestion de la sécurité des données ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 4 | Compétences en matière de communication et de présentation pour assurer la compréhension et l'adoption des politiques de sécurité par les agents et les parties prenantes de l’organisation ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 5 | Connaissance approfondie des réglementations et législations en matière de sécurité des systèmes d'information, telles que le RGPD, la loi relative à la protection de la vie privée, etc. ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 6 | Expérience dans la mise en place et la gestion de systèmes de gestion de la sécurité de l'information (ISMS) et de la certification ISO 27001 ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 7 | Bonne compréhension des besoins et des enjeux de sécurité des Pouvoirs locaux, ainsi que de leurs structures et de leurs processus opérationnels ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 8 | Capacité à établir une stratégie de sécurité adaptée aux besoins et aux contraintes des Pouvoirs locaux, en prenant en compte leurs objectifs et leurs ressources ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 9 | Connaissance de l'ensemble des domaines de la sécurité de l'information, tels que la sécurité des réseaux, de la donnée, de l'application, de l'accès, de l'identité, etc. ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 10 | Capacité à communiquer de manière claire et concise sur les politiques de sécurité et à les adapter aux différents publics cibles (personnels, utilisateurs, autorités, etc.). | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |

**Critère d’attribution 2.2 Qualité des méthodologies et documentations**

Pour chaque question posée, le soumissionnaire apporte une réponse complète et détaillée, si la réponse fait référence à une annexe (comme un rapport transmis à titre d’exemple) le tableau fait clairement apparaître la référence de l’annexe joint à la soumission afin de prendre en considération ce complément d’information. Chaque réponse sera évaluée individuellement, la somme des résultats obtenus sera utilisée pour effectuer la comparaison endogène entre les différents soumissionnaires.

| **#** | **Qualité des méthodologies et documentations** | **Conformité** | **Réponse** |
| --- | --- | --- | --- |
| 1 | Pouvez-vous décrire votre approche pour évaluer les exigences et réglementations en matière de sécurité de l'information applicables au Pouvoir local ? | Oui - Non |  |
| 2 | Quelles sont les meilleures pratiques que vous considérez comme essentielles lors de la rédaction de politiques de sécurité de l'information ? | Oui - Non |  |
| 3 | Comment proposez-vous de fournir des recommandations sur les contrôles de sécurité adaptés aux actifs de l'organisation ? | Oui - Non |  |
| 4 | Présentez et décrivez des exemples concrets de politiques de sécurité que vous avez rédigées pour des organisations similaires au Pouvoir local. | Oui - Non |  |
| 5 | Comment assurez-vous le suivi et la mise à jour régulière des politiques de sécurité de l'information ? | Oui - Non |  |
| 6 | Comment gardez-vous vos connaissances à jour concernant les réglementations et normes en matière de sécurité de l'information, telles que le RGPD, ISO 27001, NIS 2, etc. ? | Oui - Non |  |
| 7 | Comment adaptez-vous les politiques de sécurité aux besoins spécifiques du Pouvoir local en tenant compte de sa taille, de son secteur d'activité et de ses obligations réglementaires ? | Oui - Non |  |
| 8 | Quelles approches utilisez-vous pour communiquer et sensibiliser efficacement les agents aux politiques de sécurité ? | Oui - Non |  |
| 9 | Comment intégrez-vous les politiques de sécurité dans les processus de gestion de l'organisation et les systèmes informatiques ? | Oui - Non |  |
| 10 | Comment évaluez-vous et mettez-vous à jour régulièrement les politiques de sécurité pour suivre les changements dans l'environnement de sécurité ? | Oui - Non |  |
| 11 | Détaillez les formations ou certifications spécifiques que votre équipe possède (ont suivies) en matière de rédaction de politiques de sécurité de l'information. | Oui - Non |  |
| 12 | Comment collaborez-vous avec les équipes de sécurité et de gestion des Pouvoirs locaux pour établir des politiques de sécurité adaptées à leurs besoins ? | Oui - Non |  |
| 13 | Comment assurez-vous la conformité aux réglementations et normes de sécurité lors de la rédaction des politiques ? | Oui - Non |  |
| 14 | Comment abordez-vous les différents besoins et contraintes des Pouvoirs locaux en termes de politiques de sécurité de l'information ? | Oui - Non |  |
| 15 | Comment mesurez-vous l'efficacité des politiques de sécurité mises en place et quels sont les indicateurs de performance clés que vous utilisez ? | Oui - Non |  |

Lot A2 - Évaluation des vulnérabilités et « pen tests »

**Critère d’attribution 2.1 - Maîtrise des domaines d’expertise**

Le niveau d’expertise attendu des experts est décrit ci-après selon une catégorisation des domaines d'expertise. Une profil qui n’atteint pas 75% des compétences attendues sera déclaré irrégulier, ceci entraînant son exclusion du marché, si le profil exclu rend le nombre d’experts insuffisant au regard des critères de sélection qualitative, l’offre du soumissionnaire sera écartée, pour le lot concerné.

Le curriculum vitae soumis doit attester de la maîtrise des domaines revendiqués. Dans ce tableau, utilisé pour évaluer le 2ème critère d’attribution, le soumissionnaire indique dans chaque compétence marquée comme détenue l’expérience professionnelle du CV relative à ce domaine d’expertise.

| **#** | **Domaines d'expertise** | **Expert 1 - N° de CV** | **Expert 2 - N° de CV** | **Expert 3 - N° de CV** |
| --- | --- | --- | --- | --- |
| 1 | Connaissance approfondie des normes et des réglementations en matière de sécurité de l'information, comme ISO 27001 et NIS 2. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 2 | Expérience de la mise en place de programmes de gestion des vulnérabilités pour les entreprises ou les organisations publiques. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 3 | Expérience de la réalisation d'évaluations de vulnérabilités pour les systèmes d'information, les systèmes cloud, les systèmes IoT et les systèmes industriels. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 4 | Expérience dans l'utilisation des outils de détection de vulnérabilités automatisés et manuels. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 5 | Expérience en matière de sécurité des systèmes cloud (AWS, Azure, O365, etc.). | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 6 | Expérience dans la formation des employés à la sécurité de l'information. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 7 | Expérience dans la mise en place de programmes de test d'intrusion et d'évaluation des risques. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 8 | Expérience dans la gestion de la réponse aux incidents de sécurité. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 9 | Certifications ou accréditations pertinents en matière de sécurité de l'information. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 10 | Expérience dans la fourniture de rapports et de recommandations détaillées pour remédier aux vulnérabilités et réduire les risques. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |

**Critère d’attribution 2.2 Qualité des méthodologies et documentations**

Pour chaque question posée, le soumissionnaire apporte une réponse complète et détaillée, si la réponse fait référence à une annexe (comme un rapport transmis à titre d’exemple) le tableau fait clairement apparaître la référence de l’annexe joint à la soumission afin de prendre en considération ce complément d’information. Chaque réponse sera évaluée individuellement, la somme des résultats obtenus sera utilisée pour effectuer la comparaison endogène entre les différents soumissionnaires.

| **#** | **Qualité des méthodologies et documentations** | **Conformité** | **Réponse** |
| --- | --- | --- | --- |
| 1 | Décrivez les outils de détection de vulnérabilités que vous utilisez et leur méthode de sélection. | Oui - Non |  |
| 2 | Comment procédez-vous pour identifier les vulnérabilités dans les systèmes d'information des Pouvoirs locaux, y compris les systèmes cloud ? | Oui - Non |  |
| 3 | Quelles sont vos approches pour utiliser à la fois des outils automatisés et manuels dans l'évaluation des vulnérabilités ? | Oui - Non |  |
| 4 | Comment évaluez-vous les risques associés aux vulnérabilités identifiées et comment fournissez-vous des recommandations pour les remédier ? | Oui - Non |  |
| 5 | Comment assurez-vous le suivi pour vérifier que les vulnérabilités identifiées ont été corrigées et comment évaluez-vous de nouveau les risques après la mise en place des remèdes ? | Oui - Non |  |
| 6 | Explicitez comment vous sensibiliser, lors des formation, les employés des Pouvoirs locaux, aux vulnérabilités et aux bonnes pratiques de sécurité. | Oui - Non |  |
| 7 | Comment utilisez-vous les normes ISO 27001 et NIS 2 dans l'identification des vulnérabilités dans les systèmes d'information des Pouvoirs locaux ? | Oui - Non |  |
| 8 | Décrivez votre approche pour fournir des rapports de vulnérabilités détaillés et des recommandations pour remédier aux vulnérabilités identifiées. | Oui - Non |  |
| 9 | Comment procédez-vous pour offrir des services de test d'intrusion afin de vérifier la résistance des systèmes aux attaques réelles ? | Oui - Non |  |
| 10 | Comment proposez-vous des services de gestion de vulnérabilités pour aider les Pouvoirs locaux à suivre et à gérer les vulnérabilités identifiées ? | Oui - Non |  |
| 11 | Quelles sont vos compétences en matière de gestion de la réponse aux incidents de sécurité et comment aidez-vous les Pouvoirs locaux à planifier et à gérer efficacement les incidents ? | Oui - Non |  |
| 12 | Présentez et explicitez des cas concrets de rapports de vulnérabilités que vous avez produits avec des recommandations pour remédier aux vulnérabilités identifiées. | Oui - Non |  |
| 13 | Comment adaptez-vous vos méthodologies et outils en fonction des spécificités des systèmes d'information des Pouvoirs locaux wallons ? | Oui - Non |  |
| 14 | Comment garantissez-vous la confidentialité et la sécurité des informations sensibles collectées lors de l'évaluation des vulnérabilités ? | Oui - Non |  |
| 15 | Comment assurez-vous une communication efficace avec les équipes des Pouvoirs locaux lors de l'identification des vulnérabilités et de la proposition de recommandations ? | Oui - Non |  |

Lot A3 - Campagne de test de phishing/vishing/social engineering

**Critère d’attribution 2.1 - Maîtrise des domaines d’expertise**

Le niveau d’expertise attendu des experts est décrit ci-après selon une catégorisation des domaines d'expertise. Une profil qui n’atteint pas 75% des compétences attendues sera déclaré irrégulier, ceci entraînant son exclusion du marché, si le profil exclu rend le nombre d’experts insuffisant au regard des critères de sélection qualitative, l’offre du soumissionnaire sera écartée, pour le lot concerné.

Le curriculum vitae soumis doit attester de la maîtrise des domaines revendiqués. Dans ce tableau, utilisé pour évaluer le 2ème critère d’attribution, le soumissionnaire indique dans chaque compétence marquée comme détenue l’expérience professionnelle du CV relative à ce domaine d’expertise.

| **#** | **Domaines d'expertise** | **Expert 1 - N° de CV** | **Expert 2 - N° de CV** | **Expert 3 - N° de CV** |
| --- | --- | --- | --- | --- |
| 1 | Connaissance approfondie des techniques de phishing, vishing et social engineering pour comprendre les méthodes employées par les cybercriminels. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 2 | Expérience en conception et réalisation de campagnes de sensibilisation pour informer les utilisateurs sur les risques et les bonnes pratiques de prévention. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 3 | Compétences en évaluation de la vulnérabilité aux attaques de phishing pour conduire des campagnes de test et évaluer la réaction des utilisateurs. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 4 | Connaissance des bonnes pratiques de sécurité pour prévenir les attaques de phishing, vishing et social engineering et conseiller les utilisateurs sur les mesures de protection à adopter. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 5 | Expérience en formation sur les bonnes pratiques de sécurité pour sensibiliser les utilisateurs aux risques et leur enseigner les actions à prendre pour se protéger. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 6 | Connaissance des outils de détection et de prévention des attaques de phishing, vishing et social engineering pour recommander et mettre en œuvre des solutions technologiques de protection. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 7 | Évaluation de l'efficacité des campagnes de formation et de prévention pour mesurer l'engagement des utilisateurs et l'impact des mesures de sensibilisation. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 8 | Maîtrise des techniques de collecte d'informations et d'analyse des incidents de phishing, vishing et social engineering pour identifier les schémas d'attaque et prendre des mesures correctives. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 9 | Connaissance des réglementations et des normes relatives à la protection des données personnelles, telles que le RGPD, pour garantir la conformité lors de la collecte et du traitement des données. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 10 | Capacité à élaborer des rapports détaillés sur les campagnes de phishing, vishing et social engineering, incluant des recommandations pour améliorer la sécurité et renforcer la résilience des utilisateurs face à ces attaques. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |

**Critère d’attribution 2.2 Qualité des méthodologies et documentations**

Pour chaque question posée, le soumissionnaire apporte une réponse complète et détaillée, si la réponse fait référence à une annexe (comme un rapport transmis à titre d’exemple) le tableau fait clairement apparaître la référence de l’annexe joint à la soumission afin de prendre en considération ce complément d’information. Chaque réponse sera évaluée individuellement, la somme des résultats obtenus sera utilisée pour effectuer la comparaison endogène entre les différents soumissionnaires.

| **#** | **Qualité des méthodologies et documentations** | **Conformité** | **Réponse** |
| --- | --- | --- | --- |
| 1 | Comment assurez-vous que la campagne de sensibilisation aux techniques de phishing, vishing et social engineering répond aux objectifs de renforcement de la culture de sécurité et de prévention des attaques ? | Oui - Non |  |
| 2 | Décrivez les sujets abordés lors de la formation sur le phishing, le vishing et le social engineering. | Oui - Non |  |
| 3 | Quelles sont les méthodes pédagogiques utilisées pour rendre la formation interactive et participative ? | Oui - Non |  |
| 4 | Comment évaluez-vous l'efficacité de la formation et son impact sur les compétences et les pratiques des agents ? | Oui - Non |  |
| 5 | Comment garantissez-vous la qualité et la pertinence de la formation dispensée, ainsi que le suivi et l'évaluation continus ? | Oui - Non |  |
| 6 | Comment recueillez-vous les résultats de chaque campagne (taux de clics sur les liens malveillants, taux de réussite aux tests de sensibilisation, etc.) ? | Oui - Non |  |
| 7 | Quelles recommandations proposez-vous pour améliorer la protection contre les phishings, le vishing et les autres types d'attaques de social engineering ? | Oui - Non |  |
| 8 | Comment assurez-vous la continuité des connaissances acquises par les utilisateurs à long terme ? | Oui - Non |  |
| 9 | Décrivez et explicitez des exemples concrets d'attaques réussies et échouées montrées lors de formations, ainsi que les leçons à tirer de ces cas. | Oui - Non |  |
| 10 | Comment effectuez-vous une analyse des tendances et des menaces émergentes dans le domaine du phishing, du vishing et du social engineering ? | Oui - Non |  |
| 11 | Pouvez-vous présenter des études de cas ou des cas pratiques pour illustrer les enjeux de la cybersécurité spécifiques aux Pouvoirs locaux ? | Oui - Non |  |
| 12 | Comment intégrez-vous la prévention du phishing, du vishing et du social engineering dans la stratégie de cybersécurité globale des Pouvoirs locaux ? | Oui - Non |  |
| 13 | Quels rapports détaillés et documents de suivi fournissez-vous pour chaque campagne de prévention et de formation menée ? Présentez et décrivez les documents ainsi que leur constitution. | Oui - Non |  |
| 14 | Comment mesurez-vous le nombre de personnes formées et quels sont les détails de leur formation (thèmes abordés, durée, etc.) ? | Oui - Non |  |
| 15 | Comment adaptez-vous les supports de formation aux besoins spécifiques des utilisateurs, tels que des guides de sensibilisation et des présentations PowerPoint ? | Oui - Non |  |

Lot A4 - Cyber Threat Intelligence

**Critère d’attribution 2.1 - Maîtrise des domaines d’expertise**

Le niveau d’expertise attendu des experts est décrit ci-après selon une catégorisation des domaines d'expertise. Une profil qui n’atteint pas 75% des compétences attendues sera déclaré irrégulier, ceci entraînant son exclusion du marché, si le profil exclu rend le nombre d’experts insuffisant au regard des critères de sélection qualitative, l’offre du soumissionnaire sera écartée, pour le lot concerné.

Le curriculum vitae soumis doit attester de la maîtrise des domaines revendiqués. Dans ce tableau, utilisé pour évaluer le 2ème critère d’attribution, le soumissionnaire indique dans chaque compétence marquée comme détenue l’expérience professionnelle du CV relative à ce domaine d’expertise.

| **#** | **Domaines d'expertise** | **Expert 1 - N° de CV** | **Expert 2 - N° de CV** | **Expert 3 - N° de CV** |
| --- | --- | --- | --- | --- |
| 1 | Analyse de menaces: Connaissance des différentes méthodes d'analyse des menaces et des techniques utilisées pour identifier les attaques ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 2 | Intelligence artificielle et analyse de données: Connaissance de l'utilisation de l'intelligence artificielle et de l'analyse de données pour détecter les menaces et identifier les tendances ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 3 | Cryptographie: Connaissance des différents algorithmes de chiffrement et des protocoles de sécurité pour protéger les données ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 4 | Réglementation et conformité: Connaissance des normes et des réglementations en matière de sécurité de l'information et de la cybersécurité ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 5 | Ingénierie de sécurité: Connaissance des techniques d'ingénierie de sécurité pour identifier les vulnérabilités et les faiblesses dans les systèmes et les réseaux ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 6 | Veille des menaces: Connaissance des techniques et des outils pour surveiller les menaces en temps réel et identifier les tendances ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 7 | Anonymisation des données: Connaissance des techniques pour protéger les données des utilisateurs et respecter leur vie privée ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 8 | Connaissance de la réglementation en matière de données: Connaissance de la réglementation en matière de protection des données et de respect des normes en vigueur comme le RGPD ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 9 | Connaissance des systèmes de détection d'intrusion (IDS) et de prévention d'intrusion (IPS) pour protéger les systèmes et les réseaux ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 10 | Connaissance des systèmes de gestion de la sécurité (SMS) pour gérer les systèmes et les réseaux de manière sécurisée ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 11 | Connaissance des systèmes de chiffrement pour protéger les données sensibles ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 12 | Connaissance des systèmes de gestion des vulnérabilités pour identifier les faiblesses dans les systèmes et les réseaux ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 13 | Connaissance des systèmes de détection de la compromission de l'identité pour identifier les comptes compromis ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 14 | Connaissance des systèmes de gestion des configurations pour garantir la conformité aux normes de sécurité ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 15 | Connaissance des systèmes de gestion des patches pour maintenir les systèmes à jour et corriger les vulnérabilités ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 16 | Connaissance des systèmes de gestion des logs pour suivre les activités sur les systèmes et les réseaux ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 17 | Connaissance des normes et des référentiels en matière de cybersécurité tels que ISO 27001, NIST, etc. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |

**Critère d’attribution 2.2 Qualité des méthodologies et documentations**

Pour chaque question posée, le soumissionnaire apporte une réponse complète et détaillée, si la réponse fait référence à une annexe (comme un rapport transmis à titre d’exemple) le tableau fait clairement apparaître la référence de l’annexe joint à la soumission afin de prendre en considération ce complément d’information. Chaque réponse sera évaluée individuellement, la somme des résultats obtenus sera utilisée pour effectuer la comparaison endogène entre les différents soumissionnaires.

| **#** | **Qualité des méthodologies et documentations** | **Conformité** | **Réponse** |
| --- | --- | --- | --- |
| 1 | Comment garantissez-vous la mise en place d'un système de détection des intrusions efficace pour détecter les attaques à un stade précoce ? | Oui - Non |  |
| 2 | Pouvez-vous décrire les fonctionnalités et les processus utilisés dans votre système d'analyse des données de menace pour identifier les tendances et les campagnes d'attaque en cours ? | Oui - Non |  |
| 3 | Comment assurez-vous une notification rapide des menaces détectées aux Pouvoirs locaux grâce à votre système de gestion des alertes ? | Oui - Non |  |
| 4 | Comment garantissez-vous une réponse rapide et efficace aux attaques grâce à votre système de gestion des incidents ? | Oui - Non |  |
| 5 | Comment intégrez-vous votre solution de Cyber Threat Intelligence avec les systèmes de sécurité existants des Pouvoirs locaux pour une protection renforcée ? | Oui - Non |  |
| 6 | Pouvez-vous présenter le portail web que vous fournissez pour accéder aux données de menace et aux alertes en temps réel ? | Oui - Non |  |
| 7 | Comment assurez-vous la fourniture régulière de rapports sur les menaces détectées et les actions prises pour les contrer ? | Oui - Non |  |
| 8 | Pouvez-vous fournir un plan de gestion des menaces détaillant vos processus et vos outils pour surveiller les menaces et répondre aux attaques ? | Oui - Non |  |
| 9 | Quelles sont les fonctionnalités clés et les exigences techniques spécifiées dans vos cahiers des charges pour les systèmes et les outils proposés ? | Oui - Non |  |
| 10 | Comment garantissez-vous la performance, la disponibilité et la scalabilité des systèmes et des outils proposés ? | Oui - Non |  |
| 11 | Pouvez-vous fournir des scénarios d'utilisation décrivant comment vos systèmes et vos outils seront utilisés pour protéger les Pouvoirs locaux contre les menaces cybers ? | Oui - Non |  |
| 12 | Pouvez-vous présenter des études de cas et des références clients pour démontrer les résultats obtenus avec vos systèmes et vos outils ? | Oui - Non |  |
| 13 | Quelles certifications et conformités aux normes et aux réglementations en vigueur pouvez-vous fournir pour vos systèmes et vos outils, tels que les certifications ISO 27001 ou SOC 2 ? | Oui - Non |  |
| 14 | Comment assurez-vous la garantie et la maintenance des systèmes et des outils proposés ? | Oui - Non |  |
| 15 | Quels sont les supports de formation et de support que vous fournissez pour faciliter l'utilisation et la gestion des systèmes et des outils proposés ? | Oui - Non |  |

Lot A5 - Accompagnement DPD/DPO à la demande

**Critère d’attribution 2.1 - Maîtrise des domaines d’expertise**

Le niveau d’expertise attendu des experts est décrit ci-après selon une catégorisation des domaines d'expertise. Une profil qui n’atteint pas 75% des compétences attendues sera déclaré irrégulier, ceci entraînant son exclusion du marché, si le profil exclu rend le nombre d’experts insuffisant au regard des critères de sélection qualitative, l’offre du soumissionnaire sera écartée, pour le lot concerné.

Le curriculum vitae soumis doit attester de la maîtrise des domaines revendiqués. Dans ce tableau, utilisé pour évaluer le 2ème critère d’attribution, le soumissionnaire indique dans chaque compétence marquée comme détenue l’expérience professionnelle du CV relative à ce domaine d’expertise.

| **#** | **Domaines d'expertise** | **Expert 1 - N° de CV** | **Expert 2 - N° de CV** | **Expert 3 - N° de CV** |
| --- | --- | --- | --- | --- |
| 1 | Connaissance approfondie des règlementations en matière de protection des données personnelles, notamment le RGPD ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 2 | Expérience pratique en matière de mise en œuvre de politiques et de procédures de protection des données ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 3 | Connaissance des méthodes et outils de gestion des incidents de protection des données ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 4 | Compétences en matière de sensibilisation et de formation du personnel sur les bonnes pratiques en matière de protection des données ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 5 | Connaissance des techniques de sécurité des données telles que le chiffrement, la gestion des accès, la sauvegarde des données, etc. ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 6 | Expérience en matière de traitement de demandes d'exercice des droits des personnes concernées et de gestion des notifications d'incident de protection des données ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 7 | Connaissance des normes nationales et internationales de sécurité ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |

**Critère d’attribution 2.2 Qualité des méthodologies et documentations**

Pour chaque question posée, le soumissionnaire apporte une réponse complète et détaillée, si la réponse fait référence à une annexe (comme un rapport transmis à titre d’exemple) le tableau fait clairement apparaître la référence de l’annexe joint à la soumission afin de prendre en considération ce complément d’information. Chaque réponse sera évaluée individuellement, la somme des résultats obtenus sera utilisée pour effectuer la comparaison endogène entre les différents soumissionnaires.

| **#** | **Qualité des méthodologies et documentations** | **Conformité** | **Réponse** |
| --- | --- | --- | --- |
| 1 | Comment comptez-vous fournir des services de protection des données personnelles adaptés aux besoins des Pouvoirs locaux ? | Oui - Non |  |
| 2 | Pouvez-vous décrire l'expertise et la qualification de votre personnel en matière de protection des données personnelles ? | Oui - Non |  |
| 3 | Quels critères de sélection rigoureux mettez-vous en place pour vos prestataires de services liés à la protection des données personnelles ? | Oui - Non |  |
| 4 | Comment vous engagez-vous à assurer la protection des données personnelles des citoyens ? | Oui - Non |  |
| 5 | Quels mécanismes avez-vous prévus pour suivre et mesurer la qualité des services fournis en matière de protection des données personnelles ? | Oui - Non |  |
| 6 | Comment assurez-vous une formation continue pour les employés des Pouvoirs locaux sur les questions de protection des données personnelles ? | Oui - Non |  |
| 7 | Pouvez-vous démontrer votre compétence en matière de protection des données personnelles grâce à des projets précédents ou des certifications spécifiques ? | Oui - Non |  |
| 8 | Comment avez-vous mis en œuvre des politiques de protection des données et assuré la conformité avec les réglementations applicables dans des projets similaires ? | Oui - Non |  |
| 9 | Comment établissez-vous des relations de confiance avec les employés et les différentes parties prenantes pour garantir la protection des données personnelles ? | Oui - Non |  |
| 10 | Comment approfondissez-vous votre compréhension des processus de traitement des données et des mécanismes de protection des données personnelles ? | Oui - Non |  |
| 11 | Pouvez-vous partager des expériences de gestion d'incidents de protection des données et de résolution de conflits liés à la protection des données ? | Oui - Non |  |
| 12 | Comment décrivez-vous vos méthodologies et vos processus de travail pour assurer la protection des données personnelles ? | Oui - Non |  |
| 13 | Pouvez-vous fournir des échantillons de rapports précédents sur des projets similaires pour évaluer la qualité de votre travail en tant que DPD à la demande ? | Oui - Non |  |
| 14 | Quelles actions concrètes avez-vous menées pour améliorer la protection de la vie privée des personnes concernées dans des projets antérieurs ? | Oui - Non |  |
| 15 | Comment garantissez-vous la conformité avec les réglementations applicables en matière de protection de la vie privée en utilisant des outils et des technologies spécifiques ? | Oui - Non |  |

Lot A6 - RSSI as a service

**Critère d’attribution 2.1 - Maîtrise des domaines d’expertise**

Le niveau d’expertise attendu des experts est décrit ci-après selon une catégorisation des domaines d'expertise. Une profil qui n’atteint pas 75% des compétences attendues sera déclaré irrégulier, ceci entraînant son exclusion du marché, si le profil exclu rend le nombre d’experts insuffisant au regard des critères de sélection qualitative, l’offre du soumissionnaire sera écartée, pour le lot concerné.

Le curriculum vitae soumis doit attester de la maîtrise des domaines revendiqués. Dans ce tableau, utilisé pour évaluer le 2ème critère d’attribution, le soumissionnaire indique dans chaque compétence marquée comme détenue l’expérience professionnelle du CV relative à ce domaine d’expertise.

| **#** | **Domaines d'expertise** | **Expert 1 - N° de CV** | **Expert 2 - N° de CV** | **Expert 3 - N° de CV** |
| --- | --- | --- | --- | --- |
| 1 | Capacité à réaliser des évaluations de risques de sécurité et à fournir des plans d'actions détaillés pour les atténuer ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 2 | Capacité à élaborer et à fournir des formations et des sensibilisations en matière de sécurité de l'information aux employés des Pouvoirs locaux wallons ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 3 | Connaissance des pratiques et des technologies émergentes en matière de sécurité de l'information ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 4 | Expérience en gestion de la sécurité de l'information dans des environnements complexes et/ou réglementés ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 5 | Connaissance des normes et des bonnes pratiques en matière de sécurité de l'information, telles que ISO 27001 ou CIS Critical Security Controls ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 6 | Connaissance des réglementations en matière de protection des données, telles que le RGPD et la directive NIS ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 7 | Capacité à analyser les risques de sécurité de l'information et à recommander des mesures d'atténuation appropriées ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 8 | Expérience en matière de gestion d'incidents de sécurité de l'information, y compris la préparation, la réponse et la récupération ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 9 | Connaissance des technologies de sécurité de l'information, telles que les pare-feu, les antivirus, les IDS/IPS, la gestion des identités et des accès, etc. ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 10 | Connaissance des méthodologies d'évaluation de la sécurité de l'information, telles que les tests de pénétration, les tests de vulnérabilité et les évaluations de la conformité ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 11 | Capacité à élaborer et à mettre en œuvre des politiques, des procédures et des plans de sécurité de l'information. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |

**Critère d’attribution 2.2 Qualité des méthodologies et documentations**

Pour chaque question posée, le soumissionnaire apporte une réponse complète et détaillée, si la réponse fait référence à une annexe (comme un rapport transmis à titre d’exemple) le tableau fait clairement apparaître la référence de l’annexe joint à la soumission afin de prendre en considération ce complément d’information. Chaque réponse sera évaluée individuellement, la somme des résultats obtenus sera utilisée pour effectuer la comparaison endogène entre les différents soumissionnaires.

| **#** | **Qualité des méthodologies et documentations** | **Conformité** | **Réponse** |
| --- | --- | --- | --- |
| 1 | Comment comptez-vous fournir un CISO/RSSI sur demande pour assurer la gestion et la coordination de la sécurité des systèmes d'information des Pouvoirs locaux wallons ? | Oui - Non |  |
| 2 | Pouvez-vous décrire votre approche pour analyser et évaluer les risques liés aux données sensibles des Pouvoirs locaux wallons ? | Oui - Non |  |
| 3 | Comment prévoyez-vous la mise en place de plans de gestion des incidents en cas de cyberattaques et la prise en charge des actions correctives nécessaires ? | Oui - Non |  |
| 4 | Quelles méthodologies utilisez-vous pour réaliser des audits de sécurité réguliers afin d'assurer la conformité des systèmes d'information des Pouvoirs locaux wallons aux normes et standards en vigueur ? | Oui - Non |  |
| 5 | Comment accompagnez-vous les Pouvoirs locaux wallons dans la mise en œuvre de politiques de sécurité de l'information et de formation des utilisateurs ? | Oui - Non |  |
| 6 | Fournissez un exemple de plan de gestion de la sécurité de l'information que vous avez mis en place pour protéger les données et les systèmes ? | Oui - Non |  |
| 7 | Comment garantissez-vous l'efficacité des mesures de sécurité décrites dans votre plan de gestion de la sécurité de l'information ? | Oui - Non |  |
| 8 | Quelles certifications de sécurité pertinentes détenez-vous et comment ces certifications renforcent-elles votre expertise en matière de sécurité de l'information ? | Oui - Non |  |
| 9 | Illustrez et explicitez au travers de vos références clients pour des missions similaires (démontrant la portée des missions), les résultats obtenus, la qualité du service et la satisfaction du client. | Oui - Non |  |
| 10 | Comment évaluez-vous les risques et gérez-vous la sécurité de l'information, et quels outils utilisez-vous pour mener à bien ces tâches ? | Oui - Non |  |
| 11 | Comment assurez-vous la confidentialité et la sécurité des données personnelles et des données sensibles dans le cadre de vos politiques ? | Oui - Non |  |
| 12 | Comment pouvez-vous fournir des services de conseil en sécurité, y compris des audits de sécurité, des tests d'intrusion et des formations en sécurité ? | Oui - Non |  |
| 13 | Décrivez votre expérience en matière d'audit de sécurité, y compris des exemples concrets de missions réussies ? | Oui - Non |  |
| 14 | Comment assurez-vous la gestion des données personnelles et des données sensibles dans le cadre de vos activités de sécurité de l'information ? | Oui - Non |  |
| 15 | Comment garantissez-vous la qualité et l'efficacité de votre service en matière de sécurité de l'information ? | Oui - Non |  |

1. **LISTE DES POUVOIRS ADJUDICATEURS BÉNÉFICIAIRES DE LA CENTRALE D’ACHAT**

OFFRE DE PRIX POUR LE MARCHE AYANT POUR OBJET  
“ CENTRALE D'ACHAT POUR PRESTATIONS D’ACCOMPAGNEMENT EN MATIÈRE DE CYBERSÉCURITÉ ”

Procédure ouverte

| **Ville, commune** | **Type d'organisation** | **LOT A1 : Rédaction et accompagnement des politiques de sécurité** | **LOT A2 : Projet de sécurité dans le cloud** | **LOT A3 : Évaluation des vulnérabilités et pen tests** | **LOT A4 : Campagne de test de phishing/vishing/social engineering** | **LOT A5 : Cyber Threat Intelligence** | **LOT A6 : Accompagnement DPD/DPO à la demande** | **LOT A7 : RSSI as a service** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Total par lot | | 201 | 176 | 202 | 208 | 191 | 182 | 187 |
| Aiseau-Presles | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Aiseau-Presles | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Anderlues | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Anderlues | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Anhée | AC | Oui | Non | Oui | Non | Non | Non | Non |
| Anhée | CPAS | Oui | Non | Oui | Non | Non | Non | Non |
| Anthisnes | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Anthisnes | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Non | Oui |
| Arlon | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Ath | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Attert | AC | Non | Oui | Non | Oui | Oui | Non | Oui |
| Aubange | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Aubange | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Awans | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Aywaille | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Aywaille | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Bastogne | AC & CPAS | Non | Non | Non | Oui | Oui | Non | Non |
| Bastogne | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Beauvechain | AC & CPAS | Oui | Non | Oui | Oui | Non | Non | Non |
| Beloeil | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Berloz | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Bernissart | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Bièvre | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Binche | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Blégny | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Bouillon | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Boussu | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Boussu | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Braine-l'Alleud | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Braine-le-Comte | AC | Oui | Non | Non | Oui | Non | Oui | Non |
| Braine-le-Comte | CPAS | Oui | Non | Non | Oui | Non | Oui | Non |
| Brunehaut | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Cerfontaine | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Chapelle-lez-Herlaimont | AC & CPAS | Oui | Non | Oui | Oui | Non | Non | Non |
| Charleroi | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Charleroi | CPAS | Oui | Oui | Oui | Oui | Oui | Non | Oui |
| Chaudfontaine | AC & CPAS | Oui | Non | Oui | Non | Non | Non | Oui |
| Chaumont-Gistoux | AC & CPAS | Oui | Oui | Oui | Non | Oui | Non | Oui |
| Chièvres | AC | Oui | Non | Oui | Oui | Oui | Non | Oui |
| Chièvres | CPAS | Oui | Non | Oui | Oui | Oui | Non | Oui |
| Clavier | AC | Oui | Non | Non | Oui | Non | Oui | Non |
| Clavier | CPAS | Oui | Non | Non | Oui | Non | Non | Non |
| Comblain-au-Pont | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Comines-Warneton | AC | Oui | Oui | Oui | Oui | Oui | Non | Non |
| Courcelles | AC | Non | Oui | Oui | Non | Non | Oui | Non |
| Courcelles | CPAS | Non | Non | Oui | Oui | Non | Non | Oui |
| Court-Saint-Etienne | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Couvin | CPAS | Non | Non | Oui | Oui | Oui | Non | Oui |
| Daverdisse | AC | Oui | Non | Non | Oui | Non | Oui | Non |
| Daverdisse | CPAS | Oui | Non | Oui | Oui | Oui | Oui | Oui |
| Dinant | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Dison | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Dison | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Dour | AC | Non | Oui | Oui | Non | Oui | Oui | Oui |
| Dour | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Ecaussinnes | CPAS | Oui | Non | Oui | Non | Non | Oui | Non |
| Ecaussinnes | AC | Non | Oui | Oui | Oui | Oui | Oui | Non |
| Enghien | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Engis | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Engis | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Erezée | AC | Oui | Oui | Oui | Oui | Oui | Oui | Non |
| Erezée | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Non |
| Esneux | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Estaimpuis | AC & CPAS | Non | Oui | Oui | Oui | Non | Oui | Non |
| Estinnes | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Farciennes | AC | Oui | Oui | Oui | Oui | Non | Oui | Non |
| Farciennes | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Fexhe-le-Haut-Clocher | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Fleurus | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Floreffe | AC & CPAS | Non | Oui | Oui | Oui | Oui | Non | Oui |
| Florennes | AC | Oui | Non | Oui | Oui | Oui | Oui | Oui |
| Florenville | AC | Oui | Non | Non | Oui | Non | Oui | Non |
| Fosses-la-Ville | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Frameries | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Frameries | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Frasnes-lez-Anvaing | AC | Non | Non | Non | Oui | Oui | Oui | Oui |
| Froidchapelle | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Gembloux | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Genappe | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Gesves | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Gouvy | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Gouvy | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Grez-Doiceau | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Grez-Doiceau | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Habay | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Hamois | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Hastière | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Havelange | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Hélécine | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Hélécine | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Hensies | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Hensies | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Herbeumont | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Hotton | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Houffalize | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Houyet | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Huy | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Ittre | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Jalhay | AC | Oui | Non | Non | Non | Oui | Oui | Oui |
| Juprelle | CPAS | Non | Non | Non | Non | Non | Non | Non |
| Juprelle | AC | Non | Non | Non | Non | Non | Non | Non |
| Jurbise | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Jurbise | CPAS | Oui | Non | Oui | Non | Oui | Oui | Oui |
| La Bruyère | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Non | Non |
| La Hulpe | AC | Oui | Non | Oui | Oui | Oui | Oui | Oui |
| La Roche-en-Ardenne | CPAS | Oui | Non | Oui | Oui | Oui | Oui | Oui |
| La Roche-en-Ardenne | AC | Oui | Non | Oui | Oui | Oui | Oui | Oui |
| Lasne | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Lens | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Les Bons Villers | AC | Non | Oui | Oui | Oui | Oui | Non | Oui |
| Lessines | CPAS | Oui | Oui | Oui | Oui | Non | Oui | Oui |
| Leuze-en-Hainaut | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Leuze-en-Hainaut | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Libin | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Libramont-Chevigny | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Libramont-Chevigny | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Liège | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Liège | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Lierneux | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Non | Oui |
| Lincent | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Lincent | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Malmedy | AC | Oui | Non | Oui | Non | Non | Non | Non |
| Marche-en-Famenne | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Meix-devant-Virton | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Merbes-le-Château | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Merbes-le-Château | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Messancy | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Messancy | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Modave | CPAS | Oui | Oui | Oui | Oui | Oui | Non | Oui |
| Momignies | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Mont-de-l'Enclus | AC | Oui | Oui | Non | Oui | Oui | Oui | Oui |
| Mont-Saint-Guibert | AC | Oui | Oui | Oui | Oui | Oui | Non | Oui |
| Montigny-le-Tilleul | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Morlanwelz | CPAS | Non | Non | Non | Oui | Non | Oui | Oui |
| Morlanwelz | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Namur | CPAS | Oui | Non | Oui | Oui | Oui | Oui | Non |
| Namur | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Nandrin | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Nassogne | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Nassogne | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Nivelles | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Ohey | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Olne | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Onhaye | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Oreye | AC | Oui | Oui | Oui | Oui | Non | Oui | Oui |
| Ottignies-Louvain-la-Neuve | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Oupeye | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Oupeye | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Paliseul | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Péruwelz | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Perwez | AC | Oui | Oui | Oui | Non | Oui | Non | Oui |
| Perwez | CPAS | Oui | Non | Oui | Oui | Oui | Non | Oui |
| Philippeville | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Pont-à-Celles | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Profondeville | CPAS | Non | Non | Oui | Oui | Oui | Non | Non |
| Profondeville | AC | Oui | Non | Oui | Oui | Non | Oui | Oui |
| Quévy | AC | Oui | Oui | Oui | Oui | Oui | Non | Oui |
| Ramillies | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Ramillies | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Rebecq | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Rendeux | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Rendeux | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Rixensart | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Rixensart | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Rixensart | AC | Oui | Non | Oui | Oui | Non | Oui | Oui |
| Rochefort | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Rochefort | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Rouvroy | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Saint-Georges-sur-Meuse | AC & CPAS | Oui | Non | Oui | Oui | Oui | Oui | Oui |
| Saint-Ghislain | AC | Non | Oui | Non | Oui | Non | Non | Non |
| Saint-Ghislain | CPAS | Non | Oui | Non | Oui | Non | Non | Non |
| Saint-Léger (Lux.) | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Saint-Nicolas | AC | Oui | Oui | Oui | Oui | Oui | Non | Oui |
| Sainte-Ode | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Sambreville | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Sambreville | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Seneffe | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Seneffe | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Seraing | AC | Oui | Oui | Oui | Non | Oui | Oui | Non |
| Silly | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Silly | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Soignies | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Sombreffe | AC & CPAS | Oui | Non | Oui | Oui | Oui | Non | Oui |
| Somme-Leuze | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Somme-Leuze | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Stavelot | AC | Oui | Oui | Oui | Oui | Oui | Non | Oui |
| Stavelot | CPAS | Oui | Non | Oui | Oui | Oui | Non | Oui |
| Tellin | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Theux | AC | Oui | Non | Non | Non | Oui | Non | Non |
| Thimister-Clermont | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Thuin | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Tinlot | CPAS | Oui | Non | Non | Oui | Non | Non | Non |
| Tinlot | AC | Non | Non | Non | Oui | Oui | Non | Non |
| Tintigny | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Tournai | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Tournai | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Trooz | AC | Oui | Non | Oui | Oui | Non | Non | Non |
| Vaux-sur-Sûre | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Verlaine | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Verviers | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Verviers | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Villers-le-Bouillet | AC | Oui | Non | Oui | Oui | Non | Oui | Oui |
| Virton | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Virton | AC | Oui | Oui | Oui | Oui | Non | Oui | Oui |
| Visé | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Visé | CPAS | Oui | Non | Oui | Oui | Non | Non | Non |
| Waimes | AC & CPAS | Non | Non | Oui | Oui | Oui | Oui | Non |
| Walcourt | AC | Non | Non | Oui | Oui | Non | Non | Non |
| Wanze | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Waremme | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Waterloo | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Wavre | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Welkenraedt | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Wellin | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Yvoir | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Namur | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Walhain | AC | Non | Oui | Oui | Oui | Oui | Oui | Oui |
| Gesves | AC | Oui | Non | Non | Oui | Oui | Oui | Oui |
| Cerfontaine | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Chimay | AC | Non | Non | Non | Oui | Oui | Oui | Non |
| Walcourt | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Chimay | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Fléron | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Somme-Leuze | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui |

1. **RAPPORT DE LIVRAISON**

OFFRE DE PRIX POUR LE MARCHE AYANT POUR OBJET  
“ CENTRALE D'ACHAT POUR PRESTATIONS D’ACCOMPAGNEMENT EN MATIÈRE DE CYBERSÉCURITÉ ”

Procédure ouverte

Le rapport de livraison doit au minimum contenir les éléments suivants et être transmis à iMio après signature pour réception par le PAB. Aucune prestation ou livraison ne faisant pas l’objet d’un rapport de livraison complété tel que demandé et signé par le représentant du fonctionnaire dirigeant du PAB ne peut faire l’objet d’une facturation.

Titre : RAPPORT DE LIVRAISON

Coordonnées PAB

* AC-CPAS de XYZ
* Rue N°
* CP Commune
* Date adhésion à la CA Cybersécurité
* Fonctionnaire dirigeant et identification de son représentant

Coordonnées Attributaire

* Nom de société
* Rue N°
* CP Commune

Centrale d’achat : “ CENTRALE D'ACHAT POUR PRESTATIONS D’ACCOMPAGNEMENT EN MATIÈRE DE CYBERSÉCURITÉ ”

Références dossier :

* N° de marché / centrale d’achat
* N° de bon de commande PAB
* N° de devis réalisé par le prestataire

Ci-après dénommé le client : "Nom du PAB”

* Le client, représenté par la personne de contact " Fonctionnaire dirigeant et identification de son représentant“ réceptionne en date du \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ les livrables suivants avec satisfaction :
* Description des services fournis/prestés

Les anomalies ou points d’attentions suivants doivent être suivis :

* Description exhaustive des éléments nécessitant encore un suivi, ces éléments doivent être mineurs et en aucun cas n’empêcher la bonne exploitation des résultats du service

La signature de ce rapport de livraison vaut pour acceptation des matériel/logiciel/prestations dont ce rapport de livraison fait mention.

Signatures :

* Représentant fonctionnaire dirigeant PAB
* Représentant attributaire

1. **DÉLIBÉRATIONS D’ADHÉSION À LA CENTRALE D’ACHAT**

OFFRE DE PRIX POUR LE MARCHE AYANT POUR OBJET  
“ CENTRALE D'ACHAT POUR PRESTATIONS D’ACCOMPAGNEMENT EN MATIÈRE DE CYBERSÉCURITÉ ”

Procédure ouverte

Une délibération d’adhésion a été mise à disposition de tous les PAB, la voici : <https://www.imio.be/cda/cybersecurite/phase-1-audits-prealables/deliberation_conseil.docx/view>

Cette décision d’adhésion doit avoir été prise par le PAB pour que les attributaires du marché puissent leur faire une proposition dans le cadre de cette centrale d’achat.

1. **ENGAGEMENTS SUR L’OBLIGATION DE RÉSULTATS**

OFFRE DE PRIX POUR LE MARCHE AYANT POUR OBJET  
“ CENTRALE D'ACHAT POUR PRESTATIONS D’ACCOMPAGNEMENT EN MATIÈRE DE CYBERSÉCURITÉ ”

Procédure ouverte

Dans cette annexe, le soumissionnaire répond à chacun des points évoqués dans chacune des sections « Obligations de résultat » correspondante au lot soumissionné, il faut donc une annexe G par lot auquel le soumissionnaire remet une offre.

Exemple :

Chaque lot possède une section liée aux obligations de résultats, à titre d’exemple voici la section du lot A6 – RSSI as a service :

Afin d'assurer l'efficacité du service de RSSI/CISO à la demande, il est crucial de définir les obligations de résultats attendues des soumissionnaires. Les éléments suivants doivent être pris en compte lors de l'établissement de ces obligations :

* Élaboration et mise en œuvre d'un plan de sécurité adapté aux besoins de l'organisation ;
* Surveillance régulière de la sécurité des systèmes d'information et mise en place de mesures correctives en cas de violation ou de faille de sécurité ;
* Réalisation d'audits de sécurité réguliers ;
* Assistance en cas d'incidents de sécurité tels que des attaques informatiques ou des violations de données;
* Respect des normes de sécurité et des exigences légales et réglementaires ;applicables en matière de sécurité des systèmes d'information ;
* Fourniture de rapports réguliers sur l'état de la sécurité des systèmes d'information et les mesures prises pour l'améliorer ;
* Respecter les normes de sécurité en vigueur (ISO 27001, RGPD, etc.) ;
* Assurer une surveillance continue de la sécurité de l'organisation pour détecter les menaces et les incidents de sécurité le plus tôt possible ;
* Établir des plans d'actions pour résoudre les problèmes de sécurité identifiés et les mettre en œuvre dans les délais impartis.

En réponse à ces éléments, le soumissionnaire répond point par point dans cette annexe. Cet exemple doit être supprimé de la soumission.

1. La pratique des CV Vitrines est interdite [↑](#footnote-ref-0)
2. *Cfr ajout Pt III.3.1.7 du présent CSC Erratum* [↑](#footnote-ref-1)
3. *Licence à l’échelle de l’organisation – basé sur les marques d’intérêts* [↑](#footnote-ref-2)
4. *Licence à l’échelle de la personne – basé sur les marques d’intérêts* [↑](#footnote-ref-3)
5. *Licence à l’échelle de l’organisation – basé sur les marques d’intérêts* [↑](#footnote-ref-4)