Demande d'information

du

Bureau du surintendant des institutions financières

en prévision du recrutement d'un

fournisseur de services d'infogérance en sécurité

Date de publication : **15 août 2017**

Date de clôture pour la réception des réponses : **26 septembre 2017**
Numéro de référence : **OSFI MSSP-2017**

Pour toute question :

Isabelle Legault
Senior Contracting Officer
Bureau du surintendant des institutions financières
Téléphone : 613-990-6807
Courriel : contracting@osfi-bsif.gc.ca

Pour l'envoi des réponses :

Isabelle Legault
Agente principale des contrats
Bureau du surintendant des institutions financières
Courriel : contracting@osfi-bsif.gc.ca

BSIF
OSFI

DEMANDE D'INFORMATION

TABLE DES MATIÈRES

SECTION I

INTRODUCTION ET MARCHE À SUIVRE POUR RÉPONDRE À LA DEMANDE D'INFORMATION

Définition du besoin

Le Bureau du surintendant des institutions financières (BSIF) prévoit de solliciter des fonds afin d'embaucher un fournisseur de services d'infogérance en sécurité (FSIS), qui dispensera jour et nuit divers services liés aux opérations de sécurité et à la surveillance de la sécurité. Une fois approuvés le dossier de décision et les fonds s'y rattachant, le BSIF compte lancer une demande de propositions pour obtenir ces services.

L'objectif premier, ici, est d'informer les instances sectorielles des intentions du BSIF au sujet du projet FSIS et de tirer profit de leur expérience avec ce type de projet en obtenant d'elles :

a) une description de chaque service offert par les FSIS, y compris la façon dont ces services devraient normalement s'intégrer à l'architecture de sécurité et à la capacité opérationnelle du BSIF;

b) un ordre de grandeur approximatif du coût de la mise en œuvre et de l'exploitation des services, ce qui aidera le BSIF à obtenir les fonds dont il a besoin.

Contexte

Le BSIF est le principal organisme de réglementation des institutions financières à charte fédérale et des régimes de retraite fédéraux. Il a pour mission de protéger les droits et les intérêts des déposants, des souscripteurs, des participants des régimes de retraite et des créanciers des institutions financières, ainsi que de promouvoir et d'administrer un cadre de réglementation qui permet au public d'avoir confiance dans un système financier concurrentiel. Le BSIF réglemente et surveille toutes les banques, de même que l'ensemble des sociétés d'assurances, des sociétés de fiducie et de prêt, des associations coopératives de crédit, des sociétés de secours mutuel et des régimes de retraite constitués ou enregistrés sous le régime des lois fédérales.

Le BSIF se préoccupe de plus en plus de la cybersécurité, si bien qu'il est devenu important non seulement de prévenir les attaques, mais aussi de détecter, de contenir et d'éliminer les menaces qui

pèsent sur ses réseaux, et ce, par l'exercice d'un contrôle et la détection et la prévention des intrusions, et en veillant à la sécurité et à la protection de ses systèmes d'information.

Au BSIF, la fonction chargée de la cybersécurité assure divers services de sécurité internes, tels que l'élaboration des politiques, la formation et la sensibilisation à la sécurité, la gestion du risque, l'assurance sécurité logicielle et la gestion des incidents. À l'heure actuelle, le Centre des opérations de sécurité (COS), y compris la fonction chargée des rapports sur les opérations de sécurité et la surveillance de la sécurité, relève du directeur de la Division de l'infrastructure et des services technologiques. Dans le cadre de la préparation de l'analyse de rentabilisation, il est prévu de procéder à l'examen de l'ensemble des responsabilités fonctionnelles et des sources de fonds rattachées à ces activités.

Le BSIF prévoit faire appel à un seul prestataire de services professionnels pour assurer la mise en place, la gestion, l'exploitation et le maintien des services du COS et des technologies connexes, afin de prévenir et détecter les menaces à la cybersécurité et intervenir au besoin. Entre autres services de base, assurés jour et nuit, qu'il compte acquérir par le biais de la demande de propositions, citons la collecte de renseignements et l'établissement de rapports sur les menaces, le contrôle des réseaux et la classification des événements de sécurité, des services d'analyse et d'alerte, ainsi que des services d'intervention et de soutien en cas d'incidents informatiques. D'autres services pourraient être inclus dans le champ de la demande, tels qu'un soutien sur place pour la gestion des incidents, l'évaluation continue des vulnérabilités, la gestion des technologies en sécurité (pare-feu, dispositifs de sécurité du périmètre et des terminaux, etc.) et le soutien technique, ainsi que des services d'investigation judiciaire dans le cadre de la réalisation d'enquêtes.

Sur le site Web du BSIF (www.osfi-bsif.gc.ca), vous trouverez des informations détaillées sur sa mission et ses objectifs et sur son historique, sa structure organisationnelle et ses méthodes de régulation.

Nature de la demande d'information

La présente demande n'est pas un appel à soumissions et ne donnera pas lieu à l'attribution d'un contrat. Les fournisseurs éventuels des biens et services décrits aux présentes ne devraient pas réserver des stocks ou des installations ni affecter de ressources en fonction des renseignements présentés ici. De plus, la présente demande d'information ne donnera pas lieu à la création d'une liste de fournisseurs présélectionnés; par conséquent, le fait qu'un fournisseur réponde ou non à cette consultation ne l'empêchera aucunement de participer à toute autre demande ultérieure en lien avec ce projet. En outre, l'acquisition des biens et services décrits ici n'aura pas forcément lieu. La présente demande vise simplement à recueillir des informations pertinentes des instances sectorielles.

BSIF
OSFI

Communication des réponses

1. **Date d'envoi et destinataire des réponses.** Les instances sectorielles devraient faire parvenir leur réponse par courriel à la responsable mentionnée ci-après. Les réponses doivent être reçues au plus tard à la date indiquée en page 1.

2. **Ponctualité.** Les répondants doivent veiller individuellement à ce que leur réponse parvienne à temps à l'adresse prévue. Tel qu'il est indiqué précédemment, les réponses peuvent être transmises par voie électronique.

3. **Identification adéquate des réponses.** Chaque répondant doit indiquer clairement dans la réponse son nom et son adresse ainsi que le numéro de référence et la date de clôture.

4. **Retour des réponses.** Les réponses à la présente demande d'information ne seront pas retournées.

5. **Teneur des réponses.**
    a. Les répondants doivent répondre aux questions de la section III en utilisant la même numérotation.
    b. On rappelle aux répondants qu'il s'agit d'une demande d'information et non d'un appel d'offres et que, à cet égard, ils sont priés d'exprimer leurs préoccupations et de faire des commentaires et, s'il y a lieu, des recommandations concernant la façon dont les exigences ou les objectifs décrits dans le présent document pourraient être satisfaits. Les informations promotionnelles ou de marketing contenues dans les réponses ne seront pas examinées.
    c. Les réponses ne serviront pas à des fins d'évaluation concurrentielle ou comparative; toutefois, pour faciliter les choses et tirer le meilleur parti des réponses reçues, le BSIF s'attend à ce que les répondants suivent la structure décrite ci-après.

Coût de préparation des réponses

Le BSIF ne remboursera pas les répondants pour les dépenses engagées dans la préparation des réponses.

Traitement des réponses

1. **Utilisation des réponses.** Les réponses ne seront pas formellement évaluées. Toutefois, elles pourraient guider le BSIF dans la préparation ou la modification de l'analyse de rentabilisation du projet FSIS ou dans la formulation des stratégies d'approvisionnement et des exigences de la demande de propositions. Le BSIF examinera toutes les réponses obtenues avant la date de clôture et pourrait, à sa discrétion, étudier celles reçues après cette date.

2. **Équipe d'examen.** Une équipe composée de représentants du BSIF examinera les réponses. Pour l'évaluation, le BSIF se réserve le droit de faire appel à un consultant indépendant ou à des ressources de l'administration publique s'il le juge nécessaire. Tous les membres de l'équipe n'examineront pas forcément toutes les réponses.

3. **Confidentialité.** Les répondants doivent marquer les passages de leur réponse qu'ils considèrent confidentiels. Le BSIF en tiendra compte dans la mesure permise par la *Loi sur l'accès à l'information*.

4. **Suivi.** Le BSIF peut, à sa discrétion, communiquer avec un représentant pour lui poser des questions supplémentaires ou pour clarifier un point d'une réponse. Il peut aussi, s'il le juge à propos, demander une réunion à huis clos avec les répondants pour discuter de leur réponse à cette consultation et de leurs recommandations.

Demandes de renseignements

Comme il ne s'agit pas d'un appel à soumissions, le BSIF ne répondra pas forcément aux demandes de renseignements par écrit en faisant circuler ses réponses à tous les éventuels répondants. Durant la consultation, le BSIF ne répondra qu'aux questions se rapportant au processus de consultation. Il ne donnera aucune autre information concernant le projet FSIS, hormis celles données ici. Les répondants qui ont des questions au sujet de la présente consultation doivent s'adresser à la responsable suivante :

Isabelle Legault
Agente principale des contrats
Bureau du surintendant des institutions financières Canada
255, rue Albert, 12e étage Ottawa (Ontario) K1A 0H2
Téléphone : 613-990-6807
Télécopieur : 613-990-0081
Courriel : contracting@osfi-bsif.gc.ca

Calendrier préliminaire de recrutement du FSIS

Le BSIF compte lancer sa demande de propositions pour l'embauche d'un fournisseur de services d'infogérance en sécurité (FSIS) au quatrième trimestre de 2017-2018. À noter qu'il s'agit là d'une estimation qui n'est fournie qu'à titre informatif. Le BSIF se réserve le droit exclusif de modifier ce calendrier comme bon lui semble.

BSIF
OSFI

SECTION II

Étendue des travaux et informations générales sur le projet de recrutement

Contexte du projet de recrutement d'un FSIS

La vision stratégique du projet FSIS consiste à « acquérir des services liés aux opérations de sécurité et à la surveillance de la sécurité et à remplacer entièrement le centre des opérations de sécurité (COS) par quelque chose de mieux ». Il s'agit notamment d'effectuer une analyse des lacunes afin de déterminer les moyens et les technologies nécessaires, de mettre sur pied et en place ces moyens pour l'obtention de services permanents liés aux opérations de sécurité et à la surveillance de la sécurité.

Étendue des travaux

Dans le cadre de l'éventuel processus de demandes de propositions, le BSIF chercherait à embaucher un seul fournisseur pour assurer la mise en place, la gestion, l'exploitation et le maintien d'un COS évolué, afin que le BSIF puisse prévenir et détecter les menaces à la cybersécurité, intervenir et se remettre des attaques. Entre autres services de base, assurés jour et nuit, qu'il compte acquérir par le biais de la demande de propositions, citons la collecte de renseignements et l'établissement de rapports sur les menaces, le contrôle des réseaux et la classification des événements de sécurité, des services d'analyse et d'alerte, ainsi que des services d'intervention et de soutien en cas d'incidents informatiques. D'autres services pourraient être inclus dans le champ de la demande, tels qu'un soutien sur place pour la gestion des incidents, la gestion des technologies en sécurité (pare-feu, dispositifs de sécurité du périmètre et des terminaux, etc.) et le soutien technique, l'évaluation continue des vulnérabilités, ainsi que des services judiciaires pour soutenir la réalisation d'enquêtes. D'autres services encore pourraient y être inclus, par exemple, la réalisation de tests d'intrusion, d'évaluations et de tests de conformité, d'investigations numériques et d'analyses de maliciels.

Opérations de sécurité et surveillance de la sécurité

1. Effectuer, jour et nuit, le contrôle, l'analyse et la communication des alertes de sécurité et des informations d'événements qui proviennent de tous les fils de sécurité approuvés.
2. Enquêter et déterminer avec certitude les événements anormaux détectés par les dispositifs de sécurité ou signalés aux services de sécurité du BSIF par des entités externes, des administrateurs de système ou des membres de la communauté des utilisateurs.
3. Informer les parties prenantes, aviser les échelons supérieurs et produire des rapports sommaires quotidiens en se fondant sur les renseignements recueillis sur les menaces et sur l'analyse des événements de sécurité.
4. Exploiter, gérer, mettre à niveau et configurer en continu toutes les technologies de sécurité, y compris le système de gestion des informations et des événements de sécurité (GIES), les systèmes de détection et de prévention des intrusions, et d'autres technologies de sécurité pouvant faire partie du COS et des opérations de sécurité.
5. Contrôler et analyser les données sur les événements de sécurité afin de procéder à des enquêtes sur les incidents signalés à l'aide des journaux des systèmes, de la corrélation d'événements entre systèmes de détection des intrusions (SDI), de mesures de prévention de perte de données, de pare-feu et d'autres moyens de détection.
6. Examiner les journaux d'audit et consigner toute activité inappropriée ou illégale afin de reconstituer les événements survenus pendant un incident de sécurité. Cela comprend le

contrôle des réseaux et des dispositifs d'accueil et le signalement des incidents au personnel du BSIF chargé de la cybersécurité.
7. Procéder à une analyse et à une évaluation des événements de l'incident signalé et assurer la catégorisation, la priorisation et la recommandation des mesures de confinement.
8. Documenter toutes les activités d'enquête d'événements, les demandes d'information reçues ou les rapports d'incident présumés, au besoin, pour appuyer le processus de gestion des incidents du BSIF.
9. Fournir des rapports écrits détaillant tous les événements de sécurité et soumettre ces rapports dans le respect des procédures établies et des exigences en matière de rapports.

Soutien en gestion des incidents, investigation numérique et analyse de maliciels

1. Assurer, sur place et au besoin, la coordination des mesures de gestion des incidents de sécurité informatique, des interventions et des mesures de soutien à la remise en marche.
2. Effectuer des analyses techniques avancées d'activités potentiellement malveillantes qui ont ou qui pourraient avoir eu lieu dans le réseau du BSIF, en se servant des données sur les événements de sécurité du COS.
3. Proposer des recommandations correctives et produire un rapport exhaustif sur les constatations.
4. Effectuer des investigations numériques sur terminaux/ordinateurs hôtes, et des analyses de la mémoire.
5. Procéder au triage et à l'analyse approfondie et à la rétroanalyse des maliciels de Windows et des courriels d'hameçonnage, et des autres exploitations faites par des applications client, afin de faciliter la résolution des incidents de sécurité.
6. Effectuer des investigations numériques sur les médias liés aux hôtes compromis afin d'évaluer l'étendue et la nature des intrusions.
7. Assurer un soutien à distance en gestion des incidents, comme la collecte de données d'investigation, le suivi des corrélations pour détecter les intrusions, l'analyse des menaces et des tâches de correction directe des systèmes pour les intervenants sur place.
8. Tirer profit des outils d'investigation en vente sur le marché et des outils libres (p. ex., Encase) pour effectuer efficacement des analyses d'investigation.
9. Désosser l'ordre des événements d'une intrusion ou d'une attaque.
10. Effectuer une analyse statique et dynamique des fichiers pour déterminer les caractéristiques, l'intention et l'origine des maliciels.
11. Recommander des contre-mesures aux maliciels et aux autres applications et codes malveillants qui exploitent les ordinateurs hôtes, les terminaux, les réseaux et les systèmes de communication de données du BSIF.
12. Formuler des recommandations pour changer les politiques et les procédures, qui renforceront la capacité de l'infrastructure réseau du BSIF d'investiguer sur les incidents liés aux maliciels.
13. Procéder à l'analyse avancée des codes malveillants détectés sur le réseau du BSIF, y compris l'analyse hors ligne dans un environnement de laboratoire isolé dans les locaux du contractant.
14. Effectuer l'analyse avancée du trafic (au niveau des paquets) et la reconstruction du trafic réseau afin de découvrir les anomalies et les diverses tendances touchant les réseaux du BSIF.
15. Fournir des moyens avancés de détection des intrusions; créer, tester et déployer des signatures de corrélation SDI et GIES personnalisées; contrôler les dispositifs de saisie quotidienne de paquets spécialisés sur lesquels ces signatures sont apposées.

Évaluation continue de la vulnérabilité et examen de l'assurance de la sécurité

1. Effectuer des évaluations périodiques de la vulnérabilité (mensuelles et ad hoc) selon un calendrier directeur approuvé par l'équipe du BSIF chargée de la cybersécurité.

2. Coordonner d'avance les tests d'évaluation de la vulnérabilité avec l'équipe chargée de la cybersécurité afin de réduire au minimum les interruptions des travaux de maintenance, de la disponibilité et du fonctionnement prévus du réseau.
3. Utiliser les procédures de tests approuvées, les scripts et les outils d'évaluation de la vulnérabilité, y compris les dernières versions des outils dotés de listes à jour des contrôles de vulnérabilité, adaptés aux politiques, aux besoins et aux technologies du BSIF.
4. Effectuer des tests spécialisés d'évaluation de la vulnérabilité sur les bases de données et les applications Web, des tests d'intrusion et des tests et des analyses sur les technologies sans fil dans le cadre des activités prévues d'assurance de la sécurité ou des demandes de changement pour les systèmes et l'architecture, nouveaux ou modifiés.
5. Préparer et soumettre à l'approbation les règles d'engagement avant la réalisation des tests d'intrusion.
6. Procéder à un balayage ad hoc ou d'urgence des vulnérabilités pour soutenir la réalisation d'investigations ciblées réalisées à la suite d'incidents, les communications aux échelons supérieurs et les mesures d'intervention, conformément aux procédures écrites.
7. Préparer des rapports, des constatations et des recommandations pour combler les lacunes et les vulnérabilités en matière de sécurité, et soutenir l'équipe chargée de la cybersécurité en interprétant les résultats des balayages et en recommandant des plans de correction.
8. Produire des rapports sommaires sur les tests d'évaluation de la vulnérabilité, et documenter les résultats des tests.

Analyse des menaces et renseignement

1. Détecter, surveiller, analyser et atténuer les menaces ciblées, très organisées ou sophistiquées.
2. Rendre compte de la situation de l'activité et des risques auxquels le BSIF et l'administration publique sont exposés.
3. Tirer parti de toutes les sources de renseignement pour produire de l'information sur les cybermenaces, et effectuer des analyses techniques avancées des incidents qui se produisent sur les réseaux du BSIF.
4. Procéder à une analyse consolidée et complète des données et informations sur les menaces obtenues auprès de diverses sources afin de fournir des indications et des avertissements d'attaques imminentes contre les réseaux du BSIF.
5. Fournir des rapports sur les vecteurs techniques d'attaque des réseaux et des ordinateurs hôtes, sur l'émergence de cybermenaces, sur les nouvelles vulnérabilités et sur les tendances courantes utilisées par les acteurs malveillants.
6. Créer et tenir à jour des bases de données au catalogue et faire le suivi des menaces permanentes pour les réseaux du BSIF.

Tenir à jour et exploiter les technologies de sécurité

1. Veiller à ce que tous les systèmes et applications du COS soient accessibles et opérationnels.
2. Veiller à la consignation des flux de sécurité appropriés et de la corrélation dans l'outil GIES du COS.
3. Tenir à jour le système GIES afin de recueillir et d'agréger les données SDI des capteurs de réseau, les données brutes provenant des agents de collecte, des pare-feu, du serveur cache et du filtrage de contenu, du programme de prévention de la perte de données (PPD), des logiciels antivirus et des éléments du dispositif de balayage des vulnérabilités.
4. Effectuer l'administration, la gestion et la configuration des outils du COS (p. ex., GIES, SDI et PPD, dispositifs et systèmes d'application, serveurs et capteurs dédiés).
5. Élaborer les signatures des dispositifs de sécurité, les rapports sur le rendement et les mesures.

6. Synchroniser les événements du système GIES et des SDI/SPI afin de minimiser le nombre de faux positifs.
7. Installer ou modifier les composantes, les outils et les autres systèmes de sécurité du réseau, au besoin, afin de maintenir une couverture et un rendement optimaux

Documentation et procédures opérationnelles normalisées

1. Créer des diagrammes des déploiements de sécurité nouveaux ou révisés, avant qu'ils soient entre les mains du service du soutien opérationnel. Cette documentation doit englober tous les systèmes et toutes les applications qui comprennent et appuient le COS.
2. Élaborer des procédures standard d'exploitation et les réviser lorsque des changements sont apportés aux opérations du COS.
3. Produire des rapports écrits quotidiens, hebdomadaires et mensuels consistant en un résumé de toutes les activités du COS, des mesures du rendement, de l'état de la sécurité et des mesures prises pour la période.
4. Soumettre les rapports suivants à l'équipe chargée de la cybersécurité :
    a) rapports mensuels de la gestion du programme, sur les progrès réalisés durant la période courante;
    b) rapports sur les activités prévues et sur les problèmes et questions, avec les solutions recommandées;
    c) rapports sur les retards prévus et les ressources dépensées.

Période du contrat

Le BSIF prévoit d'attribuer un contrat pluriannuel comportant une période initiale et une ou plusieurs périodes optionnelles.

BSIF
OSFI

SECTION III

QUESTIONS AUX INSTANCES SECTORIELLES

Les répondants doivent à tout le moins aborder les questions suivantes :

Stratégie et méthode de mise en œuvre du COS

1) Compte tenu des renseignements fournis et d'après votre expérience de projets similaires;
    i. Quelles sont, selon vous, les principales difficultés liées au projet proposé?
    ii. Quels conseils pouvez-vous donner sur la façon de structurer une demande de propositions ou sur le mécanisme contractuel qui permettrait d'atténuer le risque associé à ces difficultés?
2) À quelles politiques et à quelles normes votre entreprise souscrit-elle et comment la conformité est-elle mesurée?
3) Quelles sont les plus grandes difficultés auxquelles un FSIS peut faire face au moment de mettre en œuvre les services du COS pour un client, et que recommanderiez-vous aux clients de faire pour minimiser les répercussions possibles avant d'externaliser leur COS?
4) On s'attend à ce que les services professionnels fassent partie de la demande de propositions pour évaluer l'environnement du BSIF et préparer un plan de travail définissant l'étendue des travaux, avant la mise en œuvre des services et des systèmes. Décrivez l'approche que vous adopteriez à cet égard.
5) Pourriez-vous décrire brièvement les divers services qu'un FSIS peut offrir à un client potentiel et ce que pourrait comporter chaque service.
6) Acquisition de technologies :
    i. En général, qui achète, implante, configure et soutient les technologies requises dans le cadre d'un arrangement avec un FSIS?
    ii. Quelles sont les technologies les plus couramment utilisées par les FSIS lorsqu'il s'agit de fournir des services liés aux opérations de sécurité, à la surveillance de la sécurité et à la gestion des incidents?
    iii. Quelle technologie, le cas échéant, est achetée, gérée, exploitée et soutenue par le client (le cas échéant)?
    iv. Pourquoi est-il avantageux pour le client de gérer cette technologie par opposition au FSIS?
7) Quels services/technologies/fonctions, le cas échéant, le BSIF devrait-il avoir en mis en place et bien rôdés avant d'externaliser le COS?
8) Pouvez-vous expliquer ou justifier pourquoi il peut être financièrement logique pour une entreprise d'externaliser le COS plutôt que de développer la fonction en interne? Vous pouvez aussi fournir des données financières ventilées à l'appui de votre argumentation.

Ententes sur les niveaux de services (ENS)

9) Quelles catégories de niveaux de services devraient être prises en compte pour assurer une capacité de détection, d'analyse et de production de rapports efficace?
10) Y a-t-il eu des obligations liées à des ENS que votre entreprise a eu de la difficulté à respecter dans le passé? Pourquoi?
11) Pouvez-vous fournir un exemple d'une ENS type que vous avez mise en place avec vos clients?
12) Comment réagiriez-vous si des incidents n'étaient pas signalés dans les délais prévus dans l'ENS?

BSIF
OSFI

Mesures, rendement et rapports du COS

13) Quelles mesures sont utilisées pour mesurer le rendement du COS et/ou pour fournir à vos clients et comment les présentez-vous à vos clients?
14) Quelle méthode recommanderiez-vous pour intégrer les mesures aux ententes contractuelles?
15) Veuillez fournir un échantillon des mesures de rendement type et un modèle de rapport au client.

Compétences et dotation en personnel

16) Quelles accréditations et quel niveau de scolarité exigez-vous des analystes de votre COS et du personnel de gestion des incidents? Quelles accréditations minimales le client devrait-il être en droit de s'attendre chez les analystes du COS?
17) Embauchez-vous différents niveaux d'analystes et, dans l'affirmative, quelles sont les exigences minimales (années d'expérience, scolarité, types de compétences) requises pour chaque niveau?
18) Votre entreprise a-t-elle habituellement recours à des sous-traitants ou maintient-elle en place des ressources internes pour répondre aux besoins de vos clients? Si vous faites appel à la sous-traitance, quel plan avez-vous mis en place pour vous assurer que des ressources suffisantes sont disponibles en tout temps pendant le contrat?
19) Si vous conservez des ressources internes, comment fidélisez-vous le personnel? Des salaires concurrentiels, des primes, d'autres formes de rémunération?
20) Offrez-vous une formation spécialisée à votre personnel du COS? Dans l'affirmative, veuillez décrire le niveau de formation, une estimation des coûts annuels, le nombre de jours alloués par employé par année, etc.
21) Le BSIF exige que tous les employés et les contractants qui travaillent auprès du COS aient une habilitation de sécurité de niveau secret du gouvernement du Canada. Cela fera-t-il problème au moment de sous-traiter des services à un FSIS?
22) Quel ratio du nombre d'employés du COS par dispositif contrôlé est considéré comme typique chez un FSIS?
23) Est-ce que les FSIS ont habituellement du personnel ayant des compétences et une expérience particulières affecté à des rôles particuliers?
24) Quelles compétences sont les plus demandées chez vos analystes du COS et quelle est votre stratégie pour vous assurer que votre personnel acquiert ou conserve ces compétences?

Budget et calendrier du projet

25) D'après l'information qui a été fournie, pouvez-vous donner une estimation approximative (–25 %/+75 %) des coûts initiaux ponctuels du projet de recrutement d'un FSIS. Donnez aussi une estimation approximative de ce qu'il en coûterait annuellement/en permanence.
26) Selon l'information fournie, combien de temps environ faudra-t-il globalement pour que le FSIS devienne entièrement opérationnel?
27) Le BSIF préférerait pouvoir tirer parti d'un contrat à prix fixe. Cela est-il faisable avec un FSIS?
28) Lorsque de nouvelles technologies sont introduites, de quelle façon cela est-il pris en compte dans les coûts annuels du contrat?
29) Comment les changements apportés aux services sont-ils pris en compte dans le prix annuel? Par exemple, peut-on ajouter des dispositifs ou des sources de données au contrat sans modifier le prix ou les services?

BSIF
OSFI

Services de gestion des incidents

30) Les FSIS acceptent-ils habituellement les provisions sur honoraires pour la gestion des incidents, telles que les interventions sur place, l'analyse des maliciels, les activités d'atténuation, les investigations? Dans l'affirmative, pouvez-vous décrire comment ce service fonctionne, y compris les divers niveaux et catégories de services offerts.
31) Pouvez-vous fournir une estimation approximative du prix pour chaque catégorie?
32) Lorsqu'il est fait appel aux services d'un FSIS qui accepte les provisions sur honoraires, comment celui-ci établit-il l'ordre de priorité des clients en cas d'incident? Cela dépend-il du niveau ou de la catégorie du service, ou le client se voit-il affecter une équipe dédiée qui dispensera ces services dans un délai prédéfini dans le contrat ou l'ENS?

Stockage des données

33) Quelles données sur les clients seront recueillies/saisies dans les systèmes du FSIS et où seront-elles stockées? Comment l'information sera-t-elle sauvegardée et où est-elle stockée habituellement? Est-ce que les FSIS utilisent habituellement des centres de secours immédiats, intermédiaires et graduels pour leur capacité de reprise sur sinistre?
34) Combien de données sont habituellement conservées par le FSIS (c.-à-d. limites de taille et de temps)?
35) Les systèmes et le lieu de stockage sont-ils réservés à un client particulier ou sont-ils partagés entre plusieurs clients?
36) Afin de respecter les obligations des politiques, les données du BSIF doivent rester au Canada et ne peuvent être stockées ou sauvegardées ailleurs. Les FSIS peuvent-ils satisfaire à cette exigence? Comment le BSIF peut-il obtenir l'assurance que cette exigence sera respectée pendant toute la durée du contrat?

Technologies et tendances

37) Est-il habituel que le client ait accès à distance en mode lecture seulement aux données du journal qui lui appartiennent et qui sont hébergées dans les systèmes du FSIS pour permettre la gestion des incidents, ou l'accès à ces données est-il habituellement réservé exclusivement au personnel compétent du FSIS?
38) Quels systèmes appartenant au client le FSIS intègre-t-il habituellement?
39) Où les technologies requises dans le cadre de ce contrat sont-elles situées (locaux du client ou locaux du FSIS)?
40) Vos services nécessiteront-ils l'utilisation de technologies exclusives que le BSIF devra acheter ou installer? Dans l'affirmative, énumérez toute l'information pertinente liée à ces technologies, y compris le matériel, les logiciels, le réseautage, les intergiciels et les exigences de base de données.
41) Le FSIS autorise-t-il habituellement l'envoi de journaux en double à ses systèmes et à ceux du client (c.-à-d. un système GIES ou un autre serveur de journalisation sur le site du client)?
42) Quels sont vos principaux secteurs d'investissement en technologie pour un COS aujourd'hui?
43) Quels investissements technologiques de pointe seront pertinents pour un COS d'ici les cinq prochaines années?
44) Quelles nouvelles techniques sont utilisées par les FSIS pour détecter les menaces persistantes évoluées et intervenir?

BSIF
OSFI

Autres commentaires

45) Avez-vous d'autres commentaires ou recommandations à faire pour nous aider à planifier ou à préparer l'éventuelle demande de proposition ou l'externalisation de notre COS?