Article #: 030030	Date: 15 Novembre 2011
Article Name: Question d'évaluation Nº 30 : Politique de sécurité	AGB Reference: none
Version #: v01	Category: Knowledge Article – Evaluation Questions

1. NOTES SUPPLÉMENTAIRES

15 Novembre 2011

1.1 Pour la question 30(a) :

- Les niveaux de sécurité sont définis par le candidat. Les candidats devront faire une liste des engagements qu'ils prendront vis-à-vis des registrants potentiels, sur la base des niveaux de sécurité définis. Il faudra fournir également une courte description de chacun des engagements mentionnés.
- Le rapport d'évaluation indépendant devra démontrer des contrôles de sécurité efficaces sur l'infrastructure IT qui sera utilisée pour exécuter les opérations de registre. La réponse du candidat devrait aborder tous les domaines traités dans le rapport d'évaluation indépendant exigeant une médiation. Veuillez noter que l'ICANN ne publiera pas le rapport d'évaluation indépendant.

1.2 Pour la question 30(b), il faudra fournir seulement une politique et des procédures de sécurité focalisées sur les opérations de registre du candidat. En raison du caractère sensible de cette information, l'ICANN ne publiera pas la politique de sécurité du candidat.

2. SUGGESTIONS DE MEILLEURES PRATIQUES :

15 Novembre 2011

2.1 Les candidats devraient lire chaque question d'évaluation dans sa totalité, y compris les notes, les critères et le texte de notation. La réponse devrait aborder tous les critères spécifiés et devrait inclure des arguments démontrant une compréhension bien approfondie du critère (c'est-à-dire, montrez votre travail).

2.2 Si des acronymes étaient utilisés, les candidats devraient énoncer clairement leur signification lors de la première mention, même si ces acronymes représentent des termes/produits/services usuels.

2.3 Les candidats qui proposent de sous-traiter une ou plusieurs fonctions de leurs opérations de registre doivent aborder les critères spécifiés dans chacune des questions pertinentes ainsi qu'inclure des arguments démontrant une compréhension bien approfondie du critère (c'est-à-dire, montrer leur travail).

2.4 La simple présentation d'un Curriculum Vitae (CV/résumé) ne sera pas considérée comme démonstration des capacités techniques ou opérationnelles ; il sera nécessaire de présenter une « preuve » démontrant que les ressources sont disponibles. Le candidat peut fournir une explication détaillée de son plan de gestion des ressources et peut inclure différents volets tels que les ressources pour gérer/exécuter une fonction, les compétences requises, le calendrier prévu, et ainsi de suite. Les CV peuvent être utilisés pour compléter le plan de gestion de ressources proposé.

2.5 Si dans une réponse les candidats font référence à une politique/procédure, ils devront fournir un résumé de cette politique/procédure. Les candidats ne présenteront pas de copies de cette politique/procédure, sauf que cela soit requis spécifiquement.

2.6 Si le candidat propose un logiciel personnalisé, il devra clarifier la portée et l'importance de cette personnalisation y compris le processus de développement du logiciel. Cette clarification vise à aider les comités d'évaluation à comprendre l'intégrité du logiciel personnalisé.

3. TEXTE DE LA QUESTION :

(a) Fournir un résumé de la politique de sécurité pour le registre proposé, incluant mais ne se limitant pas à :

- indication d'un rapport d'évaluation indépendant pour démontrer les capacités de sécurité et la prévision de rapports d'évaluation périodique indépendants pour tester les capacités de sécurité ;
- description de tous les niveaux de sécurité accrus ou des capacités en rapport avec la nature de la chaîne gTLD faisant l'objet d'une candidature, y compris l'identification des standards de sécurité internationaux ou appartenant à l'industrie que le candidat s'engage à suivre (il faudra fournir la référence du site) ;
- liste des engagements des bureaux d'enregistrement concernant les niveaux de sécurité.

Pour être éligible pour une notation de 2 points, les réponses doivent aussi inclure :

- L'évidence d'un rapport d'évaluation indépendant démontrant l'efficacité des contrôles de sécurité (par exemple, ISO 27001).

Le résumé de ce qui précède ne devrait pas dépasser les 20 pages. Veuillez noter que la politique de sécurité complète pour le registre est requise pour être soumise suivant ce étant établi dans 30(b).

(b) fournir les procédures et la politique complète de sécurité pour le registre proposé, incluant me ne se limitant pas à :

- système (données, serveur, application / services) de contrôle d'accès au réseau, garantissant une gestion sécurisée des systèmes, en incluant les détails du mode de surveillance, de consignation et de sauvegarde ;
- ressources pour assurer l'intégrité des actualisations entre les systèmes de registre et les serveurs de noms, et entre les serveurs de noms, le cas échéant ;
- rapports d'évaluation indépendants démontrant les capacités quant à la sécurité (présentés en annexe), le cas échéant ;
- mise à disposition et autres mesures permettant de réduire les risques liés aux attaques par refus de service ;
- politiques, plans et processus de réponses aux incidents informatiques et de réseau ;
- plans pour réduire au maximum le risque des accès non autorisés aux systèmes ou les interférences avec les données de registre ;
- mécanismes de détection d'intrusion, une analyse des risques du registre proposé, les défenses à développer contre ces menaces et l'actualisation périodiques des analyses de risques ;
- détails de la capacité de vérification sur tous les accès au réseau ;
- approche sécurité physique ;
- identification du département ou du groupe responsable de l'organisation de la sécurité du registre ;
- vérification des antécédents du personnel de sécurité ;
- description des principales menaces de la sécurité d'exploitation du registre ayant été identifiées.
- plans de gestion de ressources pour la mise en œuvre initiale, et la maintenance de cet aspect du critère (numéro et description des rôles du personnel destiné à ce secteur).