Rapport final de la deuxième équipe de révision de la sécurité, la stabilité et la résilience du DNS(SSR2) – Résumé analytique et recommandations

Extrait du rapport final de l’équipe de révision SSR2

1er janvier 2021

TABLE DES MATIERES

A. Résumé analytique

En vertu de l'article 4.6(c) des statuts constitutifs de la Société pour l'attribution des noms de domaines et des numéros sur Internet :

« *Le Conseil d'administration effectuera une révision périodique du respect de l'engagement de l'ICANN à renforcer la stabilité opérationnelle, la fiabilité, la résilience, la sécurité et l'interopérabilité mondiale des systèmes et processus, internes et externes qui affectent directement et / ou sont affectés par le système d'identificateurs uniques d'Internet dont l'ICANN assure la coordination (« révision de la SSR »)* ».[1]

Les révisions de la SSR sont une partie critique du mandat de l'organisation ICANN [2]de « fonctionner autant que possible de manière ouverte et transparente, conformément aux procédures conçues pour assurer l'équité ». Il s'agit de la deuxième révision de la SSR qui, en vertu des statuts constitutifs, comprend une révision par l'organisation ICANN des recommandations de la première révision de la SSR ainsi que de nouvelles recommandations pour que l'organisation ICANN les prenne en considération.

L'équipe de révision SSR2 propose 24 groupes de recommandations, ce qui donne lieu à 63 recommandations spécifiques, à commencer par l'évaluation de la réponse de l'organisation ICANN aux recommandations de la SSR1. Nous avons adopté l'approche consistant à les diviser en recommandations très spécifiques en réponse au manque de spécificité des recommandations de la SSR1. Les recommandations sont ensuite structurées de manière à offrir un aperçu des opérations internes et de l'engagement de l'organisation ICANN (en particulier les contrats et le traitement des plaintes), et de la manière dont l'organisation ICANN peut prendre des mesures pour améliorer ses propres actions SSR et aider les autres à comprendre comment améliorer les leurs. Les recommandations contenues dans le document souvent dérivent des autres et incluent des dépendances entre elles. L'organisation ICANN et le Conseil d'administration doivent en tenir compte lors de l'élaboration des plans de mise en œuvre. L'équipe de révision est parvenue à un consensus complet sur chaque recommandation.

Pour aider les futures équipes de révision SSR à faire des évaluations plus efficaces, l'équipe de révision SSR2 s'est efforcée de formuler ses propres recommandations suivant les critères SMART : *spécifiques, mesurables, attribuables, pertinentes, et traçables*. Dans de nombreux cas, les détails requis pour rendre chaque recommandation pleinement SMART, y compris l'attribution des délais appropriés, nécessiteront une réflexion et des mesures de la part de l'équipe responsable de la mise en œuvre et devraient être inclus dans le plan final de mise en œuvre. L'équipe de révision a également proposé plusieurs suggestions concernant la façon dont les révisions futures pourraient être traitées, reconnaissant que ceci ne relève pas du mandat direct de la révision SSR elle-même. Des informations supplémentaires sur le processus et la méthodologie utilisés par cette première équipe de révision SSR2 pour s'acquitter de ses responsabilités sont disponibles dans l'annexe C : Processus et méthodologie.

[1] ICANN, « Statuts constitutifs de la société pour l'attribution des noms de domaine et des numéros sur Internet : Article 4.6(c) : Révisions spécifiques : révision de la sécurité, la stabilité et la résilience » modifiée le 28 novembre, https://www.icann.org/resources/pages/governance/bylaws-en/#article4.

[2] Article 3.1 des statuts constitutifs de l'ICANN : https://www.icann.org/resources/pages/governance/bylaws-en/.

1. Contexte

Comme indiqué à la section A.2., « Objectifs de la révision de la SSR », les statuts constitutifs de l'ICANN exigent une évaluation périodique de la sécurité, la stabilité et la résilience du système des noms de domaine (DNS). Le Conseil d'administration de l'ICANN a reçu le premier rapport formel de la révision SSR le 13 septembre 2012. Cinq ans plus tard, la deuxième révision a commencé avec la réunion initiale de l'équipe de révision SSR2, tenue le 2 mars 2017. Cependant, depuis sa création, l'équipe de révision SSR2 a rencontré plusieurs défis qui ont prolongé la durée de la révision bien au-delà de ce qui était prévu. L'équipe de révision SSR2 s'est réunie régulièrement jusqu'en octobre 2017, lorsque le Conseil d'administration a interrompu ses activités.[3] Les réunions ont repris avec de nouveaux membres le 19 juin 2018.[4]

Le paysage de l'écosystème global d'identificateurs uniques a continué d'évoluer au cours de la période prolongée du processus de révision. En dépit de la perturbation mondiale des activités et des déplacements résultant de la pandémie de COVID-19 qui a entraîné des retards supplémentaires dans le processus de révision SSR2, l'équipe de révision SSR2 a pu terminer son travail. Au cours de la dernière année du processus de révision, l'équipe a choisi de ne pas recommencer l'évaluation de ses recommandations initiales, mais plutôt de préserver leurs contributions fondamentales et historiques. L'équipe de révision estime que ces recommandations restent largement pertinentes pour l'organisation ICANN et pour soutenir la sécurité, la stabilité et la résilience du DNS mondial.

2. Objectifs de la révision SSR

En conformité avec l'article 4.6(c) des statuts constitutifs de l'ICANN : *« Le Conseil d'administration effectuera une révision périodique du respect de l'engagement de l'ICANN à renforcer la stabilité opérationnelle, la fiabilité, la résilience, la sécurité et l'interopérabilité mondiale des systèmes et processus, internes et externes, qui affectent directement et / ou sont affectés par le système d'identificateurs uniques d'Internet dont l'ICANN assure la coordination (« révision SSR »)*[5].

Il indique en particulier que :

ii. L'équipe de révision SSR (« équipe de révision SSR ») pourra évaluer ce qui suit :

1. *des questions concernant la sécurité, la stabilité opérationnelle et la résilience, tant au niveau physique que du réseau, eu égard à la coordination du système d'identificateurs uniques de l'Internet ;*
2. *le respect d'un plan de mesures d'urgence approprié pour le système d'identificateurs uniques de l'Internet ;*

[3] Lettre du Dr Stephen D. Crocker, président du Conseil d'administration de l'ICANN, à l'équipe de révision SSR2, en date du 28 octobre 2017, https://www.icann.org/en/system/files/correspondence/crocker-to-ssr2-28oct17-en.pdf.

[4] ICANN, « La deuxième révision de la sécurité, la stabilité et la résilience du DNS (SSR2) recommence », blog du 7 juin 2018, https://www.icann.org/news/announcement-2-2018-06-07-en.

[5] Article 4.6(c) des statuts constitutifs de l'ICANN, https://www.icann.org/resources/pages/governance/bylaws-en.

3. *le maintien de procédures de sécurité claires et interopérables à l'échelle mondiale pour les parties du système d'identificateurs uniques de l'Internet dont l'ICANN assure la coordination.*

iii. L'équipe de révision SSR évaluera également si l'organisation ICANN a bien mis en œuvre ses actions en matière de sécurité, quelle a été l'efficacité de ses actions en matière de sécurité pour répondre aux défis et aux menaces réels et potentiels liés à la sécurité et la stabilité du DNS, et jusqu'à quel point ses actions en matière de sécurité sont suffisamment robustes pour répondre aux menaces et aux enjeux futurs liés à la sécurité, la stabilité et la résilience du DNS, et ce conformément à la mission de l'ICANN.

iv. L'équipe de révision SSR examinera également à quel point les recommandations formulées par les révisions SSR précédentes ont été mises en œuvre et dans quelle mesure la mise en œuvre de ces recommandations a abouti aux résultats escomptés.

v. La révision SSR sera menée au moins tous les cinq ans à compter de la date à laquelle s'est réunie l'équipe de révision SSR précédente ».

3. Influence des autres équipes de révision et des comités consultatifs

L'organisation ICANN devrait s'impliquer à plusieurs équipes de révision et comités consultatifs (AC), comme l'exigent les statuts constitutifs de l'ICANN. Bien que chacun de ces comités et équipes ait des mandats précis, les recommandations formulées par ces groupes peuvent se chevaucher sur les domaines de travail des autres équipes de révision et comités. L'équipe de révision SSR2 a évalué les recommandations d'autres équipes de révision et comités consultatifs afin de déterminer si leurs recommandations publiées ont eu un impact sur la sécurité, la stabilité et la résilience de l'organisation ICANN et du DNS mondial. Dans plusieurs cas, l'équipe de révision SSR2 a jugé nécessaire d'incorporer et de s'appuyer sur ces recommandations pour développer les directives relatives à la SSR pour l'organisation ICANN (voir en particulier la section E.1. Mesures de sauvegarde non atteintes pour le programme des nouveaux gTLD et la section E.3. Alternatives des PDP). L'équipe de révision SSR2 a considéré ces chevauchements sur les recommandations comme une corroboration tacite des mérites des questions correspondantes et a davantage considéré les accords entre les recommandations de l'équipe de révision et celles d'autres groupes comme un soutien empirique à leur nécessité. Les recommandations de la SSR2 sont destinées à compléter les recommandations de ces autres équipes de révision.

B. Recommandations de la SSR2

L'équipe de révision SSR2 est parvenue à un consensus complet sur chaque recommandation.

1. Tableau récapitulatif

Nº	Recommandation	Propriétaire	Priorité

Recommandation 1 de la SSR2 : révision des recommandations de la SSR1			
1.1	Le Conseil d'administration de l'ICANN et l'organisation ICANN doivent effectuer une révision plus approfondie des recommandations de la SSR1 et exécuter un nouveau plan pour achever la mise en œuvre de ces recommandations (voir l'annexe D : Conclusions relatives aux recommandations de la SSR1).	Conseil d'administration de l'ICANN et organisation ICANN	Faible
Recommandation 2 de la SSR2 : créer un poste de direction où le titulaire soit responsable de la sécurité stratégique et tactique et de la gestion des risques			
2.1	L'organisation ICANN devrait créer un poste responsable de la sécurité (CSO) ou responsable de la sécurité des informations (CISO) au niveau de la direction de l'organisation ICANN, embaucher une personne qualifiée pour ce poste et allouer un budget spécifique suffisant pour exécuter les fonctions liées à ce rôle.	Organisation ICANN	Moyenne - Élevée
2.2	L'organisation ICANN devrait inclure dans la description de ce rôle que le responsable gèrera la fonction de sécurité de l'organisation ICANN et supervisera les interactions du personnel dans tous les domaines pertinents ayant un impact sur la sécurité. Le responsable devrait être chargé de fournir des rapports réguliers au Conseil d'administration et à la communauté de l'ICANN sur toutes les activités liées à la sécurité, la stabilité et la résilience au sein de l'organisation ICANN. Les fonctions de sécurité existantes devraient être restructurées et réorganisées sur le plan organisationnel pour en informer ce nouveau directeur.	Organisation ICANN	Moyenne - Élevée
2.3	L'organisation ICANN devrait inclure dans la description de ce rôle que ce directeur sera responsable de la sécurité stratégique et tactique et de la gestion des risques. Ces domaines de responsabilité comprennent la responsabilité et la coordination stratégique d'une fonction centralisée d'évaluation des risques, la planification de la continuité des opérations (BC) et du plan de reprise après sinistre (DR) (voir également la recommandation 7 de la SSR2 : améliorer les processus et procédures de continuité des opérations et de reprise après sinistre) dans le domaine de la sécurité interne de l'organisation, y compris le serveur racine géré par l'ICANN (IMRS, communément dénommé racine-L), et coordonner avec d'autres parties prenantes impliquées dans le système	Organisation ICANN	Moyenne - Élevée

	d'identificateurs global externe, ainsi que publier une méthodologie et une approche d'évaluation des risques.		
2.4	L'organisation ICANN devrait inclure dans la description de ce rôle que ce cadre exécutif sera responsable de toutes les questions et responsabilités budgétaires liées à la sécurité et prendra part à toutes les négociations contractuelles relatives à la sécurité (par exemple, les contrats de registre et de bureau d'enregistrement, les chaînes d'approvisionnement pour le matériel et les logiciels, et les conventions de service y associées) entreprises par l'organisation ICANN, en signant toutes les conditions contractuelles liées à la sécurité.	Organisation ICANN	Moyenne - Élevée
Recommandation 3 de la SSR2 : améliorer la transparence budgétaire liée à la sécurité, la stabilité et la résilience			
3.1	Le cadre exécutif responsable de la sécurité (voir la recommandation 2 de la SSR2 : créer un poste de direction où le titulaire soit responsable de la sécurité stratégique et tactique et de la gestion des risques) devrait informer la communauté au nom de l'organisation ICANN au sujet de la stratégie, des projets et du budget SSR de l'organisation ICANN deux fois par an et mettre à jour et publier des aperçus de budget chaque année.	Organisation ICANN	Élevée
3.2	Le Conseil d'administration de l'ICANN et l'organisation ICANN devraient s'assurer que les éléments de budget spécifiques concernant la performance de l'organisation ICANN des fonctions liées à la SSR soient liés aux buts et objectifs spécifiques du plan stratégique de l'ICANN. L'organisation ICANN devrait mettre en œuvre ces mécanismes par le biais d'un processus de budgétisation et de rapport annuel cohérent et détaillé.	Conseil d'administration de l'ICANN et organisation ICANN	Élevée
3.3	Le Conseil d'administration de l'ICANN et l'organisation ICANN devraient créer, publier et demander des commentaires publics sur des rapports détaillés concernant les coûts et la budgétisation liés à la SSR dans le cadre du cycle du plan stratégique.	Conseil d'administration de l'ICANN et organisation ICANN	Élevée
Recommandation 4 de la SSR2 : améliorer les processus et les procédures de gestion des risques			
4.1	L'organisation ICANN devrait continuer à centraliser sa	Organisatio	Élevée

	gestion des risques, articuler clairement son cadre de gestion des risques de sécurité et s'assurer que cela s'aligne stratégiquement sur les exigences et les objectifs de l'organisation. L'organisation ICANN devrait décrire les mesures pertinentes de succès et la façon dont ces mesures doivent être évaluées.	n ICANN	
4.2	L'organisation ICANN devrait adopter et mettre en œuvre la norme ISO 31000 « Gestion des risques », valider et certifier sa mise en œuvre par des audits indépendants appropriés. L'organisation ICANN devrait mettre à la disposition de la communauté des rapports d'audit, potentiellement expurgés. Les efforts de gestion des risques devraient être inclus dans les plans et procédures de la BC et de la DR (voir la recommandation 7 de la SSR2 : améliorer les processus et procédures de continuité des opérations et de reprise après sinistre).	Organisation ICANN	Élevée
4.3	L'organisation ICANN devrait nommer ou désigner une personne responsable et dédiée à la gestion des risques de sécurité qui informera le cadre supérieur chargé de la sécurité (voir la recommandation 2 de la SSR2 : créer un poste de direction où le titulaire soit responsable de la sécurité stratégique et tactique et de la gestion des risques). Cette fonction devrait mettre à jour régulièrement, informer sur un registre des risques de sécurité et guider les activités de l'organisation ICANN. Les conclusions devraient être prises en compte dans les plans et les procédures de la continuité des opérations (BC) et la reprise après sinistre (DR) (voir la recommandation 7 de la SSR2 : améliorer les processus et procédures de continuité des opérations et de reprise après sinistre) et le système de gestion de la sécurité de l'information (ISMS) (voir la recommandation 6 de la SSR2 : se conformer aux systèmes de gestion de la sécurité de l'information et des certifications de sécurité).	Organisation ICANN	Élevée
Recommandation 5 de la SSR2 : se conformer aux systèmes de gestion de la sécurité de l'information et des certifications de sécurité			
5.1	L'organisation ICANN devrait mettre en œuvre un ISMS qui devrait être audité et certifié par un tiers selon les normes de sécurité de l'industrie (par exemple, ITIL, famille ISO 27000, SSAE-18) pour ses responsabilités opérationnelles. Le plan devrait inclure une feuille de route et des dates limites pour obtenir des certifications et noter les domaines qui seront la cible d'une amélioration continue.	Organisation ICANN	Élevée

5.2	Dans le cadre du ISMS, l'organisation ICANN devrait élaborer un plan de certifications et de formation pour les rôles à remplir dans l'organisation, effectuer le suivi des taux d'achèvement, justifier leurs choix et documenter la manière dont les certifications s'intègrent aux stratégies de sécurité et de gestion des risques de l'organisation ICANN.	Organisation ICANN	Élevée
5.3	L'organisation ICANN devrait exiger que les parties externes qui fournissent des services à l'organisation ICANN soient conformes aux normes de sécurité pertinentes et documentent leur diligence raisonnable concernant les fournisseurs et les fournisseurs de services.	Organisation ICANN	Élevée
5.4	L'organisation ICANN devrait informer la communauté et au-delà en présentant des rapports clairs qui démontrent ce que l'organisation ICANN fait et réalise dans le domaine de la sécurité. Ces rapports seraient extrêmement utiles s'ils fournissaient des informations décrivant comment l'organisation ICANN suit les meilleures pratiques et établit des processus peaufinés et en constante amélioration pour gérer les risques, la sécurité et les vulnérabilités.	Organisation ICANN	Élevée
Recommandation 6 de la SSR2 : divulgation et transparence de la vulnérabilité de la SSR			
6.1	L'organisation ICANN devrait promouvoir de manière proactive l'adoption volontaire des meilleures pratiques et des objectifs de la SSR pour la divulgation de la vulnérabilité par les parties contractantes. Si les mesures volontaires s'avèrent insuffisantes pour atteindre l'adoption de telles meilleures pratiques et objectifs, l'organisation ICANN devrait mettre en œuvre les meilleures pratiques et objectifs dans les contrats, les accords et les protocoles d'accord.	Organisation ICANN	Élevée
6.2	L'organisation ICANN devrait mettre en œuvre un rapport coordonné de divulgation de vulnérabilités. Les divulgations et les informations concernant les problèmes liés à la SSR, tels que les violations au sein de toute partie contractante et les cas de vulnérabilités critiques découvertes et signalées à l'organisation ICANN, doivent être communiquées rapidement aux parties de confiance et concernées (par exemple, les personnes concernées ou requises pour résoudre le problème). L'organisation ICANN devrait faire régulièrement des rapports sur les vulnérabilités (au moins une fois par an), y compris les mesures	Organisation ICANN	Élevée

	anonymisées et en utilisant une divulgation responsable.		
Recommandation 7 de la SSR2 : améliorer les processus et procédures de continuité des opérations et de reprise après sinistre			
7.1	L'organisation ICANN devrait établir un plan de continuité des opérations pour tous les systèmes appartenant à l'organisation ICANN, ou sous sa responsabilité, basé sur la norme ISO 22301 « gestion de la continuité des opérations », identifiant des délais acceptables pour la continuité des opérations et la reprise après sinistre (BC/DR).	Organisation ICANN	Moyenne - Élevée
7.2	L'organisation ICANN devrait s'assurer que le plan de reprise après sinistre pour les opérations de l'entité Identificateurs techniques publics (PTI) (c'est-à-dire les fonctions IANA) inclue tous les systèmes pertinents qui contribuent à la sécurité et à la stabilité du DNS, qui comprennent également la gestion de la zone racine et en conformité avec la norme ISO 27031. L'organisation ICANN devrait développer ce plan en étroite collaboration avec le Comité consultatif du système des serveurs racine (RSSAC) et les Opérateurs de serveur racine (RSO).	Organisation ICANN	Moyenne - Élevée
7.3	L'organisation ICANN devrait également établir un plan de reprise après sinistre pour tous les systèmes détenus par ou sous le mandat de l'organisation ICANN, toujours en conformité avec la norme ISO 27031.	Organisation ICANN	Moyenne - Élevée
7.4	L'organisation ICANN devrait établir un nouveau site pour la reprise après sinistre pour tous les systèmes appartenant à l'organisation ICANN ou sous son mandat, dans le but de remplacer les sites Los Angeles ou Culpeper ou d'ajouter un troisième site permanent. L'organisation ICANN devrait localiser ce site en dehors de la région de l'Amérique du nord et de tout territoire américain. Si l'organisation ICANN choisissait de remplacer l'un des sites existants, ce site ne devrait pas être fermé tant que l'organisation n'ait pas vérifié que le nouveau site soit entièrement opérationnel et capable de gérer la reprise après sinistre de ces systèmes pour l'organisation ICANN.	Organisation ICANN	Moyenne - Élevée
7.5	L'organisation ICANN devrait publier un résumé de ses plans et procédures pour la continuité des opérations et la reprise après sinistre à l'échelle mondiale. Cela améliorerait la transparence et la fiabilité au-delà des	Organisation ICANN	Moyenne - Élevée

	objectifs stratégiques de l'organisation ICANN. L'organisation ICANN devrait engager un auditeur externe pour vérifier les aspects liés à la conformité avec ces plans de continuité des opérations et de reprise après sinistre.		
Recommandation 8 de la SSR2 : permettre et démontrer la représentation de l'intérêt public dans les négociations avec les parties contractantes			
8.1	L'organisation ICANN devrait mettre en place une équipe de négociation comprenant des experts en matière d'abus et de sécurité non affiliés ou payés par des parties contractantes pour représenter les intérêts des entités non contractantes et travailler avec l'organisation ICANN pour renégocier les contrats des parties contractantes de bonne foi, avec transparence publique, et dans le but d'améliorer la SSR du DNS pour les utilisateurs finaux, les entreprises et les gouvernements.	Organisation ICANN	Moyenne
Recommandation 9 de la SSR2 : surveiller et appliquer la conformité			
9.1	Le Conseil d'administration de l'ICANN devrait demander à l'équipe chargée de la conformité de surveiller et d'appliquer strictement la conformité des parties contractantes aux obligations SSR actuelles et futures et aux obligations en matière d'abus dans les contrats, les accords de base, les spécifications temporaires et les politiques communautaires.	Conseil d'administration de l'ICANN	Élevée
9.2	L'organisation ICANN devrait surveiller et appliquer de manière proactive les obligations contractuelles des registres et des bureaux d'enregistrement afin d'améliorer l'exactitude des données d'enregistrement. Cette surveillance et cette application devraient inclure la validation des champs d'adresses et la réalisation de vérifications périodiques de l'exactitude des données d'enregistrement. L'organisation ICANN devrait concentrer ses efforts d'application sur les bureaux d'enregistrement et les opérateurs de registre ayant fait l'objet de plus de 50 plaintes ou rapports par an concernant la présentation de données auprès de l'organisation ICANN.	Organisation ICANN	Élevée
9.3	L'organisation ICANN devrait mener des activités de conformité auditées en externe au moins une fois par an et publier les rapports d'audit et la réponse de l'organisation ICANN aux recommandations d'audit, y compris les plans de mise en œuvre.	Organisation ICANN	Élevée

9.4	L'organisation ICANN devrait s'occuper de la fonction de conformité en publiant des rapports réguliers qui énumèrent les outils manquants qui aideraient à soutenir l'organisation ICANN dans son ensemble et à l'utilisation efficace des clauses contractuelles pour traiter les menaces de sécurité au DNS, y compris les mesures qui nécessiteraient des modifications aux contrats.	Organisation ICANN	Élevée
Recommandation 10 de la SSR2 : clarifier les définitions des termes relatifs à l'utilisation malveillante			
10.1	L'organisation ICANN devrait publier une page Web incluant sa définition pratique de l'utilisation malveillante du DNS, c'est-à-dire ce qu'elle utilise pour les projets, les documents et les contrats. La définition devrait signaler explicitement les types de menaces de sécurité que l'organisation ICANN, en vertu de son mandat, considère actuellement qu'il faut traiter par le biais de mécanismes contractuels et de conformité, ainsi que ceux qui, de l'avis de l'organisation ICANN, se trouvent en dehors de ses attributions. Si l'organisation ICANN utilisait une autre terminologie similaire, par exemple « une menace à la sécurité », « un comportement malveillant », elle devrait inclure à la fois sa définition de ces termes et la manière dont elle établit précisément une distinction entre ces termes et l'utilisation malveillante du DNS. Cette page devrait inclure des liens vers des extraits de toutes les obligations actuelles liées à l'utilisation malveillante dans les contrats avec les parties contractantes, y compris les procédures et protocoles pour répondre aux abus. L'organisation ICANN devrait mettre à jour cette page chaque année, inclure la date de la dernière version et fournir les liens vers des versions plus anciennes avec les dates de publication y associées.	Organisation ICANN	Élevée
10.2	Établir un groupe de travail intercommunautaire (CCWG) appuyé par le personnel afin d'établir un processus permettant de faire évoluer les définitions de l'interdiction de l'utilisation malveillante du DNS, au moins une fois tous les deux ans, selon un calendrier prévisible (par exemple, tous les mois de janvier), qui ne prendra pas plus de 30 jours ouvrables. Ce groupe devrait faire participer les parties prenantes de la protection des consommateurs, de la cybersécurité opérationnelle, de la recherche universitaire ou indépendante sur la cybersécurité, de l'application de la loi et du commerce électronique.	Organisation ICANN	Élevée

10.3	Le Conseil d'administration de l'ICANN et l'organisation ICANN devraient utiliser les définitions de consensus de manière cohérente dans les documents publics, les contrats, les plans de mise en œuvre de l'équipe de révision et d'autres activités, et faire en sorte que ces termes renvoient à cette page Web lorsqu'ils sont utilisés.	Organisation ICANN	Élevée
Recommandation 11 de la SSR2 : résoudre les problèmes d'accès aux données CZDS			
11.1	La communauté de l'ICANN et l'organisation ICANN devraient prendre des mesures pour assurer que l'accès au Service centralisé de données de zone (CZDS) soit disponible, en temps voulu, et qu'il n'y ait pas d'obstacles inutiles pour les demandeurs, par exemple le manque d'auto-renouvellement des informations d'identification d'accès.	Conseil d'administration de l'ICANN et organisation ICANN	Moyenne
Recommandation 12 de la SSR2 : réviser les efforts d'analyse et de signalement de l'utilisation malveillante du DNS pour permettre la transparence et la révision indépendante			
12.1	L'organisation ICANN devrait créer une équipe consultative d'analyse de l'utilisation malveillante du DNS composée d'experts indépendants (c'est-à-dire d'experts sans conflits d'intérêts financiers) pour recommander une refonte de l'activité de signalement d'abus du DNS avec des données exploitables, la validation, la transparence et la reproductibilité indépendante des analyses comme ses priorités les plus élevées.	Organisation ICANN	Moyenne
12.2	L'organisation ICANN devrait structurer ses accords avec les fournisseurs de données d'une manière qui permette le partage des données à des fins non commerciales, en particulier pour la validation ou la recherche scientifique examinée par des pairs. Cette licence non commerciale spéciale et gratuite pour utiliser les données peut impliquer un délai qui ne présente pas de conflit avec les opportunités de revenus commerciaux du fournisseur de données. L'organisation ICANN devrait publier tous les termes du contrat de partage de données sur le site Web de l'ICANN. L'organisation ICANN devrait mettre fin à tout contrat qui ne permette pas une vérification indépendante de la méthodologie derrière la liste de noms bloqués.	Organisation ICANN	Moyenne
12.3	L'organisation ICANN devrait publier des rapports qui	Organisatio	Moyenne

	identifient les opérateurs de registre et les bureaux d'enregistrement dont les domaines sont responsables de la plupart des cas d'abus L'organisation ICANN devrait inclure des formats de données lisibles par machine, en plus des données graphiques incluses dans les rapports actuels.	n ICANN	
12.4	L'organisation ICANN devrait rassembler et publier des rapports sur les actions prises par les opérateurs de registre et les bureaux d'enregistrement, soit volontaires, soit en réponse à des obligations juridiques, pour répondre à des plaintes pour conduite illégale et / ou malveillante basées sur les lois applicables en relation avec l'utilisation du DNS.	Organisation ICANN	Moyenne
Recommandation 13 de la SSR2 : accroître la transparence et la responsabilité du signalement des plaintes pour abus			
13.1	L'organisation ICANN devrait établir et entretenir un portail centralisé des plaintes sur l'utilisation malveillante du DNS qui envoie automatiquement tous les rapports d'utilisation malveillante aux parties concernées. Le système agirait purement comme un flux entrant, et l'organisation ICANN collecterait et traiterait uniquement le résumé et les métadonnées, y compris les horodatages et les types de plaintes (catégoriques). L'utilisation du système devrait devenir obligatoire pour tous les domaines génériques de premier niveau (gTLD) ; la participation de chaque domaine de premier niveau géographique (ccTLD) serait volontaire. En outre, l'organisation ICANN devrait partager les rapports d'abus (par exemple, par e-mail) avec tous les ccTLD.	Organisation ICANN	Élevée
13.2	L'organisation ICANN devrait publier le nombre de plaintes déposées sous une forme qui permette à des tiers indépendants d'analyser les types de plaintes concernant le DNS.	Organisation ICANN	Élevée
Recommandation 14 de la SSR2 : créer une spécification temporaire pour les améliorations de la sécurité fondées sur des données factuelles			
14.1	L'organisation ICANN devrait créer une spécification temporaire qui exige que toutes les parties contractantes maintiennent le pourcentage de domaines identifiés par l'activité de signalement d'abus DNS révisée (voir la recommandation 13.1 de la SSR2) comme abusive en dessous d'un seuil raisonnable et publié.	Organisation ICANN	Élevée

14.2	Pour permettre une action anti-abus, l'organisation ICANN devrait fournir aux parties contractantes des listes de domaines dans leurs portefeuilles identifiés comme abusifs, conformément à la recommandation 12.2 de la SSR2 concernant la révision indépendante des données et des méthodes pour la liste de domaines bloqués.	Organisation ICANN	Élevée
14.3	Si le nombre de domaines liés à une activité abusive atteignait le seuil publié décrit dans la recommandation 14.1 de la SSR2, l'organisation ICANN devrait mener une enquête pour confirmer la véracité des données et de l'analyse, puis émettre un avis à la partie concernée.	Organisation ICANN	Élevée
14.4	L'organisation ICANN devrait permettre aux parties contractantes un délai de 30 jours pour réduire la fraction de domaines abusifs en dessous du seuil ou pour démontrer que les conclusions ou les données de l'organisation ICANN sont erronées. Si une partie contractante ne parvenait pas à faire la rectification pendant 60 jours, le département de la conformité contractuelle de l'ICANN devrait passer au processus de désaccréditation.	Organisation ICANN	Élevée
14.5	L'organisation ICANN devrait envisager d'offrir des incitations financières : les parties contractantes avec des portefeuilles au-dessous d'un pourcentage donné de noms de domaine abusifs devraient recevoir une réduction des frais sur les transactions payantes jusqu'à un seuil approprié.	Organisation ICANN	Élevée
Recommandation 15 de la SSR2 : lancer un EPDP fondé sur des données factuelles pour améliorer la sécurité			
15.1	Après avoir créé la spécification temporaire (voir la recommandation 14 de la SSR2 : créer une spécification temporaire pour les améliorations de sécurité fondées sur des données factuelles), l'organisation ICANN devrait établir un processus accéléré d'élaboration de politiques (EPDP) soutenu par le personnel pour créer une politique anti-abus. Les volontaires de l'EPDP devraient représenter la communauté de l'ICANN, en utilisant les numéros et la distribution de la spécification temporaire pour les données d'enregistrement de gTLD comme modèle de charte de l'équipe responsable de l'EPDP.	Organisation ICANN	Élevée
15.2	L'EPDP devrait s'appuyer sur le fondement de la définition du CCWG proposée dans la recommandation 10.2 de la SSR2. Ce cadre de politique devrait définir	Organisation ICANN	Élevée

	des contre-mesures et des mesures correctives appropriées pour différents types d'abus, des délais pour les actions des parties contractantes tels que les délais des rapports d'abus/rapports de réponse et les actions d'application de la conformité contractuelle de l'ICANN en cas de violations de la politique. L'organisation ICANN devrait insister sur le pouvoir de résilier les contrats dans le cas de répétitions de conduites et de pratiques de protection des abus de la part de toute partie contractante. Le résultat devrait inclure un mécanisme de mise à jour des critères de référence et des obligations contractuelles liées aux abus tous les deux ans, en utilisant un processus qui ne prendrait pas plus de 45 jours ouvrables.		
Recommandation 16 de la SSR2 : exigences de confidentialité et RDS			
16.1	L'organisation ICANN devrait fournir des références croisées cohérentes sur son site Web afin de fournir des informations claires et faciles à trouver sur toutes les actions, passées, présentes et planifiées, prises au sujet de la confidentialité et de la gestion des données, en portant une attention particulière aux informations concernant le service d'annuaire de données d'enregistrement (RDS).	Organisation ICANN	Moyenne
16.2	L'organisation ICANN devrait créer des groupes spécialisés au sein de la fonction de conformité contractuelle qui comprennent les exigences et les principes de confidentialité (tels que la limitation de la collecte, la qualification des données, la spécification des objectifs, et des mesures de sécurité pour la divulgation) et qui puissent faciliter les besoins d'application de la loi dans le cadre du RDS, modifié et adopté par la communauté (voir également la recommandation 11 de la SSR2 : résoudre les problèmes d'accès aux données CZDS).	Organisation ICANN	Moyenne
16.3	L'organisation ICANN devrait effectuer des audits périodiques sur le respect des politiques de protection de la vie privée mises en œuvre par les bureaux d'enregistrement pour s'assurer que celles-ci aient mis en place des procédures pour traiter les atteintes à la vie privée.	Organisation ICANN	Moyenne
Recommandation 17 de la SSR2 : collision de noms			
17.1	L'organisation ICANN devrait créer un cadre qui caractérise la nature et la fréquence des collisions de	Organisation ICANN	Moyenne

	noms et des préoccupations y associées. Ce cadre devrait inclure des mesures et des mécanismes pour établir à quel point l'interruption contrôlée réussit à identifier et à éliminer les collisions de noms. Ceci peut être pris en charge par un mécanisme permettant d'activer la divulgation protégée des instances de collision de noms. Ce cadre devrait permettre le traitement approprié des données sensibles et des menaces à la sécurité.		
17.2	La communauté de l'ICANN devrait élaborer une politique claire pour éviter et gérer les collisions de noms liées à de nouveaux gTLD et mettre en œuvre cette politique avant la prochaine série de gTLD. L'organisation ICANN devrait s'assurer que l'évaluation de cette politique soit entreprise par les parties n'ayant aucun intérêt financier dans l'expansion des gTLD.	Conseil d'administration de l'ICANN et organisation ICANN	Moyenne
Recommandation 18 de la SSR2 : informer les débats sur les politiques			
18.1	L'organisation ICANN devrait suivre les avancées de la communauté de chercheurs évalués par les pairs, en se concentrant sur le réseautage et les conférences de recherche sur la sécurité, y compris au moins, ACM CCS, ACM Internet Measurement Conference, Usenix Security, CCR, SIGCOMM, le Symposium sur la sécurité et la vie privée de l'IEEE, ainsi que les conférences sur la sécurité opérationnelle et FIRST, et publier un rapport pour la communauté de l'ICANN qui résume les implications des publications qui ont trait au comportement de l'organisation ICANN ou des parties contractantes.	Organisation ICANN	Faible
18.2	L'organisation ICANN devrait assurer que ces rapports comprennent des observations pertinentes pouvant avoir trait à des recommandations d'actions, y compris les changements aux contrats avec les opérateurs de registre et les bureaux d'enregistrement, qui pourraient atténuer, prévenir ou réparer les préjudices en matière de SSR pour les consommateurs et les infrastructures identifiées dans la documentation révisée par des pairs.	Organisation ICANN	Faible
18.3	L'organisation ICANN devrait également recommander que ces rapports incluent des recommandations pour des études supplémentaires qui confirment les résultats révisés par les pairs, une description des données qui seraient nécessaires pour mener à bien d'autres études, et expliquer comment l'organisation ICANN peut offrir d'aider à garantir l'accès à de telles données,	Organisation ICANN	Faible

	par exemple, via le CZDS.		
Recommandation 19 de la SSR2 : développement complet d'un test de régression du DNS			
19.1	L'organisation ICANN devrait compléter la mise au point d'une suite de tests de comportement des résolveurs du DNS.	Organisation ICANN	Faible
19.2	L'organisation ICANN devrait garantir que la capacité de continuer à exécuter des tests fonctionnels des différentes configurations et versions de logiciel soit mise en œuvre et entretenue.	Organisation ICANN	Faible
Recommandation 20 de la SSR2 : procédures officielles pour les roulements de clé			
20.1	L'organisation ICANN devrait établir une procédure formelle, étayée sur un outil de modélisation et de langage qui suive un processus formel, pour spécifier les détails des roulements de clé futurs, y compris des points à décider, à l'exception de certains extraits, le plein contrôle du débit, etc. La vérification du processus de roulement de clé devrait inclure la publication de la procédure de programmation (par exemple, le programme ou l'automate avec un nombre défini d'états (FSM)) pour consultation publique et l'organisation ICANN devrait intégrer les commentaires de la communauté. Le processus devrait remplir des critères d'acceptation vérifiables empiriquement à chaque étape pour que le processus continue. Ce processus devrait être réévalué au moins aussi souvent que le roulement lui-même (c'est-à-dire, avec la même périodicité) de sorte que l'organisation ICANN puisse utiliser les leçons apprises pour ajuster le processus.	Organisation ICANN	Moyenne
20.2	L'organisation ICANN devrait créer un groupe de parties prenantes qui implique le personnel de l'ICANN (l'organisation ou la communauté) pour exécuter régulièrement des exercices de simulation qui suivent le processus de roulement de la KSK de la racine.	Organisation ICANN	Moyenne
Recommandation 21 de la SSR2 : améliorer la sécurité des communications avec les opérateurs de TLD			
21.1	Les opérations de l'organisation ICANN et de la PTI devraient accélérer la mise en œuvre de nouvelles mesures de sécurité du système de gestion de la zone racine (RZMS) concernant l'authentification et l'autorisation des modifications demandées et offrir aux opérateurs de TLD la possibilité de tirer parti de ces	Organisation ICANN et Conseil d'administration de l'ICANN	Moyenne

	mesures de sécurité, en particulier l'authentification MFA et les e-mails chiffrés.		
Recommandation 22 de la SSR2 : mesures du service			
22.1	Pour chaque service qui relève de l'autorité de l'organisation ICANN, y compris les services liés à la zone racine et aux gTLD, ainsi que les registres IANA, l'organisation ICANN devrait créer une liste de statistiques et de mesures qui reflètent l'état opérationnel (comme la disponibilité et la réactivité) de ce service, et publier un répertoire de ces services, ensembles de données et mesures sur une seule page du site Web icann.org, par exemple sous la plateforme de données ouvertes (ODP). L'organisation ICANN devrait produire des mesures pour chacun de ces services sous forme de résumés à la fois au cours de l'année précédente et longitudinalement (pour illustrer le comportement de base).	Organisation ICANN	Faible
22.2	L'organisation ICANN devrait demander chaque année des commentaires de la communauté sur les mesures. Cette rétroaction devrait être prise en considération, résumée publiquement après chaque rapport et incorporée dans les rapports de suivi. Les données et les méthodologies associées utilisées pour mesurer les résultats de ces rapports devraient être archivées et rendues publiques afin de favoriser la reproductibilité.	Organisation ICANN	Faible
Recommandation 23 de la SSR2 : roulement de l'algorithme			
23.1	Les opérations de la PTI devraient mettre à jour la déclaration de pratiques DNSSEC (DPS) pour faciliter la transition d'un algorithme de signature numérique à l'autre, y compris une transition précoce de l'algorithme de signature numérique RSA à d'autres algorithmes ou à des algorithmes après-quantiques futurs, ce qui créera une sécurité équivalente ou même supérieure et préservera ou améliorera la résilience du DNS.	PTI	Moyenne
23.2	Étant donné que le roulement de l'algorithme DNSKEY de la racine est très complexe et délicat, l'équipe opérationnelle de la PTI devrait travailler avec les autres partenaires de la zone racine et la communauté internationale à l'élaboration d'un plan de consensus pour les roulements futurs de l'algorithme DNSKEY de la racine, compte tenu des leçons tirées du premier roulement de la KSK de la racine en 2018.	PTI	Moyenne

Recommandation 24 de la SSR2 : améliorer la transparence et les tests de bout en bout pour le processus EBERO			
24.1	L'organisation ICANN devrait coordonner les tests de bout en bout du processus EBERO complet à des intervalles prédéterminés (au moins une fois par an) en utilisant un plan de test qui inclue des ensembles de données utilisés pour les tests, les états de progression et les délais, et qui soit coordonné à l'avance avec les parties contractantes de l'ICANN afin de garantir que toutes les exceptions soient exercées et en publier les résultats.	Organisation ICANN	Moyenne
24.2	L'organisation ICANN devrait faciliter la recherche du manuel du processus de transition commun en fournissant des liens sur le site Web de l'EBERO.	Organisation ICANN	Moyenne

2. Établissement des priorités

L'équipe de révision SSR2 a harmonisé toutes les recommandations de la SSR2 avec le plan stratégique pour les exercices fiscaux 2021 à 2025 de l'ICANN, ses buts et objectifs.[6] L'équipe de révision a retiré de ce rapport toute recommandation qui ne s'harmonise pas clairement avec le plan stratégique. Toutes les recommandations de l'équipe de révision SSR2 sont en ligne avec le plan stratégique de l'organisation ICANN et sont considérées comme importantes.

L'équipe de révision SSR2 a utilisé un outil d'enquête en ligne (la solution Qualtrics, basée sur Internet) pour interroger tous les membres de l'équipe sur la priorité de chaque groupe de recommandations dans ce rapport.[7] Cette enquête a permis de classer chaque groupe sur une échelle de cinq points, à savoir : priorité très faible, priorité faible, priorité moyenne, priorité élevée et très haute priorité.

L'équipe de révision a déterminé que sur les vingt-quatre groupes de recommandations, vingt-sept recommandations spécifiques dont la plupart concernent la gestion interne de la sécurité de l'organisation ICANN et les actions anti-abus devraient être considérées comme étant de priorité élevée. Neuf recommandations sont de priorité moyenne-élevée. Dix-huit recommandations, provenant principalement des sections mondiales du DNS, ont été classées en priorité moyenne, et les huit recommandations restantes ont été classées en priorité faible.

[6] Voir l'annexe G : Mappage des recommandations de la SSR2 pour le plan stratégique de l'ICANN des exercices fiscaux 2021 à 2025 et pour les statuts constitutifs de l'ICANN.

[7] Voir https://www.qualtrics.com/.