ICANN Organization Assessment - SSR2 Pending Recommendations
November 2022

On 22 July 2021, the Board took action on the 63 SSR2 recommendations, as issued in the SSR2 Review Team Final Report, and noted within the Scorecard titled "Final SSR2 Review Team Recommendations – Board Action." The Board placed 34 recommendations into one of three pending categories, and directed ICANN org to gather additional information including clarification from SSR2 Implementation Shepherds.

This document provides ICANN org's assessment on 21 of SSR2 pending recommendations for Board consideration. that were placed into one of following three categories; one pending, likely to be approved once further information is gathered to enable approval (20.2), five pending, likely to be rejected unless additional information shows implementation is feasible (6.1, 6.2, 7.4, 16.2, 16.3), and 15 pending, holding to seek clarity or further information (3.1, 3.2, 3.3, 4.3, 5.3, 7.1, 7.2, 7.3, 7.5, 11.1, 18.1, 18.2, 18.3, 20.1, 24.1).

<table>
<tr><th>SSR2 Recommendation</th><th>SSR2-defined measures of success</th><th>Board action</th></tr>
<tr><td>3.1: The Executive C-Suite Security Officer (see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management) should brief the community on behalf of ICANN org regarding ICANN org's SSR strategy, projects, and budget twice per year and update and publish budget overviews annually.

SSR2 designated priority: High
SSR2 designated owner: ICANN org</td><td rowspan="3">SSR2-defined measures of success for Recommendation SSR2-defined measures of success for Recommendation 3: Improve SSR-related Budget Transparency (3.1 - 3.3): This recommendation can be considered implemented when ICANN org moves all relevant functions and budget items under the new C-Suite position. This recommendation can be considered effective when the ICANN community has a transparent view of the SSR-related budget.</td><td rowspan="3">The Board notes that, as written, successful implementation of Recommendations 3.1 - 3.3 depends on implementation of Recommendation 2. The Board is rejecting Recommendation 2 on the establishment of a Chief Security Officer (CSO) or Chief Information Security Officer (CISO) at the Executive C-Suite level of ICANN org based on the rationale set out for that recommendation.

The Board directs the ICANN President and CEO, or his designee(s), to seek clarification from the SSR2 Implementation Shepherds as to the SSR2 Review Team's intent, and if implementation of these recommendations can be considered effective after the Board rejects Recommendation 2, thereby removing the possibility of assigning the additional roles or responsibilities as called for in Recommendations 3.1, 3.2, and 3.3 to that new office. The Board has a concern with accepting recommendations for which implementation can never be deemed successful or effective. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.</td></tr>
<tr><td>3.2: The ICANN Board and ICANN org should ensure specific budget items relating to ICANN org's performance of SSR-related functions are linked to specific ICANN Strategic Plan goals and objectives. ICANN org should implement those mechanisms through a consistent, detailed, annual budgeting and reporting process.

SSR2 designated priority: High
SSR2 designated owner: ICANN Board and ICANN org</td></tr>
<tr><td>3.3:The ICANN Board and ICANN org should create, publish, and request public comment on detailed reports regarding the costs and SSR-related budgeting as part of the strategic planning cycle.

SSR2 designated priority: High
SSR2 designated owner: ICANN Board and ICANN org</td></tr>
<tr><td colspan="3">22 July 2021 Board Rationale:
Recommendations 3.1, 3.2 and 3.3 pertain to responsibilities of the C-Suite position recommended in Recommendation 2 and SSR-related budget transparency. The community inputs that the Board considered when acting on this recommendation showed that while several commenters support the recommendations, RySG, i2Coalition, Namecheap, and RrSG believe that the recommendations are already being addressed, or can be sufficiently addressed within the current ICANN organization structure, without the addition of a C-Suite level position. For example:

- RySG - "RySG supports the recommended actions to improve SSR-related budget transparency, but cautions that briefings to the ICANN community on SSR strategy and projects should be high level and not disclose specific security practices, so as not to introduce potential attack vectors. We reiterate that, as per our previous comment, we do not support the creation of the Executive CSuite Security Officer referred to in Recommendation 3.1, as this role is already sufficiently being covered within ICANN Org."</td></tr>
</table>

- i2Coalition - “The Final Report is full of recommendations that, without stating the problem that is to be solved, ask for new roles that already seem to exist (2.1, 3.1, 4.3), or seem to be pushing ICANN into the realm of policing DNS protocols (19). This is a serious concern with recommendations that, once accepted by the Board, would create duplicative work, or even seem to expand ICANN’s remit.”
- Namecheap - “A number of the recommendations in the SSR2 Final Report address items or functions that ICANN org already provides- and in some cases is already dedicating significant resources toward. Specifically, Recommendations 2, 3, and 4.3 already exist within ICANN.”
- RrSG - “It is not clear to the RrSG how ICANN’s current public comment on its budget (including SSR-related items) and strategic planning is deficient to necessitate this recommendation, nor why the Review Team designated this as a high priority item.”

The Board supports increased transparency where possible, and as such agrees with the intent of these recommendations. ICANN org is already undertaking work towards improving budget transparency. For example, ICANN org’s Operating and Financial Plans for FY22-26 (Five-Year) and FY22 (One-Year), includes “Appendix C: ICANN Security, Stability, and Resiliency (SSR) of the Unique Internet Identifiers". This appendix states: “ICANN’s deep commitment to SSR underscores an approach to the concept that is holistic and interwoven into daily operations. In other words, every function of ICANN org contributes to the overall SSR through its support of org’s work to advance ICANN’s Mission. However, this Appendix aims to articulate some of the specific areas that particularly focus on supporting the SSR of these unique Internet identifiers.” Further, the Board agrees with the benefit of a process of periodic communication on SSR activities and notes this is already partially performed as part of the current annual planning process. The Board encourages ICANN org to continue enhancing its periodic communication on SSR activities as part of its work and operations.

However, the Board notes that, as written, successful implementation of Recommendations 3.1 - 3.3 depends on implementation of Recommendation 2. The Board is rejecting Recommendation 2 on the establishment of a Chief Security Officer (CSO) or Chief Information Security Officer (CISO) at the Executive C-Suite level of ICANN org based on the rationale set out for that recommendation. In light of the above considerations, the Board directs the ICANN President and CEO, or his designee(s), to seek clarification from the SSR2 Implementation Shepherds as to the SSR2 Review Team’s intent, and if implementation of these recommendations can be considered effective after the Board rejects Recommendation 2, thereby removing the possibility of assigning the additional roles or responsibilities as called for in Recommendations 3.1, 3.2, and 3.3 to that new office. The Board has a concern with accepting recommendations for which implementation can never be deemed successful or effective. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board’s decision on next steps.

SSR2 Implementation Shepherd’ responses to clarifying questions were received on 20 June 2022

“Question a - relating to 3.1, 3.2, 3.3: Given that Recommendation 2.1 was rejected by the Board, could these dependent recommendations be successfully implemented by existing ICANN org security, planning and reporting positions and Board Risk committee detailed in 22 July 2021 Board Action Scorecard and Board Rationale?

Answer a - While the Board has decided not to create the C-Suite position. A single point of responsibility for SSR-related topics is highly desirable. The implementation shepherds observe that having security report to operations goes against accepted best practices. The single point of responsibility was intended to cover strategic security, tactical security, and risk management. The suggested way forward does not accomplish this goal.

Question b - Regarding SSR2 Recommendations 3.1, ICANN org's current plan for reporting framework and engagement reflects an annual cycle of reporting with two (2) milestones of publication per year. One of these two (2) milestones has already been implemented in the form of the Appendix D to the Five Year Operating and Financial Plan for FY23-27 (pages 262-264). Is this reporting in alignment with the SSR2 Implementation Shepherds intended outcomes?

Answer b - No. There is no transparency provided by these broad statements.

Question c.i. - Regarding SSR2 Recommendations 3.2 and 3.3, SSR-related elements are included in ICANN’s Five Year Operating & Financial Plan and Annual Operating Plan and Budget, and the Five Year Strategic Plan. Extensive public consultation activities are in place with regard to these documents. See, for example, information about ICANN's strategic planning process and the most recent Public Comment proceeding on the draft Five-Year Operating & Financial Plan and draft Operating Plan & Budget.

Do the above mentioned elements generally address the intended purpose of Recommendations 3.2 and 3.3?

Answer c.i. - No. There is no transparency provided by these broad statements. Further, simply stating that an activity is "SSR related" does not allow the same insight as a specific line dedicated to SSR.

Question c.ii. - Is there additional work beyond what is already in place to meet the requirements of the recommendation?

Answer c.ii. - Yes. Much greater visibility into the SSR-related activities and the cost of each SSR-related activity is desired.”

ICANN org Assessment:

The SSR2 Review Team’s defined measures of success imply that if the C-Suite position is not in place (Recommendation 2 which the Board rejected), these recommendations would be considered not implemented regardless of the activities that ICANN org is already undertaking. For implementation of these recommendations to be considered effective, the ICANN community should have a transparent view of the SSR-related budget.

ICANN org notes that while the success for Recommendation 3.1 depends on the new C-Suite position, Recommendations 3.2 and 3.3' success should be considered independently from the C-Suite Position.

SSR budget, reporting and public comment elements referred to in the recommendations are already part of ICANN org's modus operandi. More specifically:

1. ICANN org's Operating and Financial Plans for FY 22-26 (Five-Year) and FY22 (One-Year) includes "Appendix C: ICANN Security, Stability, and Resiliency (SSR) of the Unique Internet Identifiers."
2. Periodic communication on SSR activities is part of the current annual planning process.
3. Extensive public consultation activities are in place with regard to the Five Year Operating & Financial Plan and Annual Operating Plan and Budget, and the Five Year Strategic Plan. See, for example, information about ICANN's strategic planning process and the most recent Public Comment proceeding on the draft FY22-FY26 Five-Year Operating & Financial Plan and draft Operating Plan & Budget.

Proposed Board Action: Reject Recommendations 3.1, and approve Recommendations 3.2 and 3.3 which can be considered as fully implemented.

SSR2 recommendation	SSR2-defined measures of success	Board action
4.3: ICANN org should name or appoint a dedicated, responsible person in charge of security risk management that will report to the C-Suite Security role (see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management). This function should regularly update, and report on, a register of security risks and guide ICANN org's activities. Findings should feed into BC and DR plans and procedures (see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures) and the Information Security Management System (ISMS) (see SSR2 Recommendation 6: Comply with Appropriate Information Security Management Systems and Security Certifications). **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 4: Improve Risk Management Processes and Procedures (4.1 - 4.3):** This recommendation can be considered implemented when ICANN org's risk management processes are sufficiently documented as per international standards (e.g., ISO 31000), and the organization has established a cycle of regular audits for this program that include the publication of audit summary reports. This recommendation can be considered effective when ICANN org has a strong, clearly documented risk management program.	The Board notes that as written, successful implementation of Recommendation 4.3 depends on implementation of Recommendation 2. The Board is rejecting Recommendation 2 on the establishment of a CSO or CISO at the Executive C-Suite level of ICANN org based on the rationale set out for that recommendation. In light of this dependency on Recommendation 2, the Board directs the ICANN President and CEO, or his designee(s) to seek clarification from the SSR2 Implementation Shepherds as to if implementation of this recommendation can be considered effective after the Board rejects Recommendation 2 thereby removing the possibility of assigning the additional roles or responsibilities as called for in Recommendation 4.3. The Board has a concern with accepting a recommendation for which implementation can never be deemed successful or effective. Further, the Board notes it is the responsibility of the ICANN President and CEO, or his designee(s), to structure ICANN org, and the President and CEO can only be held accountable to the management choices he structures and implements. It is not appropriate for the Board or a review team to curtail that authority or accountability. In addition, it is not clear as to what the SSR2 Review Team envisioned would be mitigated, nor what cost/benefit would be derived from the recommended structure. The Board directs the ICANN President and CEO, or his designee(s) to seek clarity from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

22 July 2021 Board Rationale:
Recommendation 4.3 recommends that ICANN org "name or appoint a dedicated, responsible person in charge of security risk management that will report to the C-Suite Security role" as recommended in Recommendation 2. The community inputs that the Board considered when acting on Recommendation 4.3 showed that while several commenters support the recommendation, , RySG, i2Coalition, Namecheap, and RrSG cite concerns about the elements of the recommendation that ask for a new role to be created that already exists in ICANN org. For example:

- RySG - “RySG is generally supportive of risk mitigation management within ICANN and believe that this can be sufficiently addressed within the current ICANN staff structures without the addition of a C-Suite level position.”
- i2Coalition - “The Final Report is full of recommendations that, without stating the problem that is to be solved, ask for new roles that already seem to exist (2.1, 3.1, 4.3), or seem to be pushing ICANN into the realm of policing DNS protocols (19). This is a serious concern with recommendations that, once accepted by the Board, would create duplicative work, or even seem to expand ICANN’s remit.”
- Namecheap - “Recommendations 2, 3, and 4.3 already exist within ICANN…It is not clear from the SSR2 Final Report whether the Review Team is aware of these ICANN activities, or how the Review Team finds these significant and beneficial activities to be insufficient.”
- RrSG - “As of the date of this comment, ICANN’s Office of the Chief Technology Officer (OCTO) comprises approximately 20 staff. It is not clear to what extent the functions identified in this recommendation are not currently performed by OCTO, or why a new position is required to perform these functions. To the extent these functions are not currently performed by OCTO, the team should be capable of incorporating these items into their existing departmental structure.”

The Board notes that as written, successful implementation of Recommendation 4.3 depends on implementation of Recommendation 2. The Board is rejecting Recommendation 2 on the establishment of a Chief Security Officer (CSO) or Chief Information Security Officer (CISO) at the Executive C-Suite level of ICANN org based on the rationale set out for that recommendation. In light of this dependency on Recommendation 2, the Board directs the ICANN President and CEO, or his designee(s) to seek clarification from the SSR2 Implementation Shepherds as to if implementation of this recommendation can be considered effective after the Board rejects Recommendation 2 thereby removing the possibility of assigning the additional roles or responsibilities as called for in Recommendation 4.3. The Board has a concern with accepting a recommendation for which implementation can never be deemed successful or effective.

Further, the Board notes it is the responsibility of the ICANN President and CEO, or his designee(s), to structure ICANN org, and the President and CEO can only be held accountable to the management choices he structures and implements. It is not appropriate for the Board or a review team to curtail that authority or accountability. In addition, it is not clear as to what the SSR2 Review Team envisioned would be mitigated, nor what cost/benefit would be derived from the recommended structure.

The Board directs the ICANN President and CEO, or his designee(s) to seek clarity from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board’s decision on next steps.

SSR2 Implementation Shepherd responses to clarifying questions were received on 20 June 2022

“Question a - Recommendation 4.3 suggests the appointment of a dedicated, responsible person in charge of security risk management, who will report to the C-Suite Security role, and update, report on and guide ICANN org's related security activities. ICANN has in place a risk management program that reports to the C-suite under the direction of the CFO. It includes, and is significantly broader than, security-related risk management. Within this program, identified risks, their assessment rating and mitigation plans, including relative to security, are reviewed regularly, updated and reported to management and to the Board Risk Committee. These existing activities would appear to address the intended outcome of the recommendation. While not performed under the C-suite responsibility suggested in the recommendation, it is carried out under an existing C-suite executive which provides the appropriate executive-level visibility and accountability. Considering that even broader activities are already being carried out than those in this recommendation, and are already under the direction of a C-level executive, do the existing activities align with the intended outcomes for this recommendation, even if not reporting to a new C-level executive requested in dependent Recommendation 2.1?

Answer a - It is the understanding of the implementation shepherds that strategic security and tactical security do not report to the CFO. As stated above, a single point of responsibility was intended to cover strategic security, tactical security, and risk management.

Question b - Given that Recommendation 2.1 was rejected, can Recommendation 4.3 be successfully implemented by existing ICANN org security, planning and reporting positions and committees detailed in Board Action Scorecard?

Answer b - At a minimum, placing strategic security, tactical security and risk management under a single point of responsibility should be done. The position needs to have the authority to place security above other demands of their time and other resources.”

ICANN org Assessment:

The Board rejected Recommendation 2 that called for the establishment of a CSO or CISO at the Executive C-Suite level of ICANN org. In light of this dependency on Recommendation 2, the Board directed the ICANN President and CEO, or his designee(s) to seek clarification from the SSR2 Implementation Shepherds as to whether implementation of this recommendation could be considered effective after the Board rejects Recommendation 2, thereby removing the possibility of assigning the additional roles or responsibilities as called for in Recommendation 4.3. Answers received from the SSR2 Implementation Shepherds do not alter the recommendation language as stated.

Considering that:

- strategic and tactical security risks are specifically assigned to a C-suite position (SVP and CIO Ashwin Rangan, also with the CISO role),
- risk management is under the responsibility of a C-suite position (SVP and CFO Xavier Calvez), with responsibility to manage all risks faced by the organization, including but not limited to security risks,
- a CEO Risk Management Committee is in place, chaired by the CEO, and includes all C-Suite executives with responsibilities to manage all areas of risk, including but not limited to security risks, and
- a Board Risk Committee oversees the management of all risks by ICANN org, including but not limited to all security risks.

Proposed Board Action: Reject

SSR2 recommendation	SSR2-defined measures of success	Board action
5.3: ICANN org should require external parties that provide services to ICANN org to be compliant with relevant security standards and document their due diligence regarding vendors and service providers. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications (5.1 - 5.4):** This recommendation can be considered implemented when ICANN org has an ISMS oriented alongside accepted standards (e.g., ITIL, ISO 27000 family, SSAE-18), with regular audits that validate the appropriate security management and management procedures. This recommendation can be considered effective when ICANN org has an Information Security Management System that is thoroughly documented and adequately addresses current security threats and offers plans to address potential future security threats.	The Board understands that ICANN org's Engineering & Information Technology (E&IT) function already requires all vendors and service providers to have a risk assessment performed and documented which meets industry-standard requirements. Based on the questions asked to and the answers received from the SSR2 Shepherds, the recommendation could be addressed by a policy that defines security standards and due diligence procedures applied to vendors and service providers. Separately, the Board reiterates that the COSO framework applied by org for risk management activities is appropriate and suitable to ICANN's needs. As a result, the Board adopts recommendation 5.3 and directs the President and CEO to design and implement a policy that enables org to evaluate the security measures in place with vendors and service providers, documents its due diligence and performs verification as is considered appropriate.

22 July 2021 Board Rationale:
Recommendation 5.3 recommends "external parties that provide services to ICANN org to be compliant with relevant security standards and document their due diligence regarding vendors and service providers." The community inputs that the Board considered when acting on Recommendation 5.3 showed commenters generally support the recommendation. The Board understands that ICANN org's Engineering & Information Technology (E&IT) function already requires all vendors and service providers to have a risk assessment performed and documented which meets industry-standard requirements. In order to accurately assess resource requirements and feasibility, the Board requires clarification from the SSR2 Implementation Shepherds as to if the SSR2 Review Team's intent was to expand this risk assessment to all ICANN org vendors and service providers. The Board directs the ICANN President and CEO, or his designee(s), to seek clarification from the SSR2 Implementation Shepherd as to the SSR2 Review Team's intended scope of this recommendation. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

SSR2 Implementation Shepherds' responses to clarifying questions were received on 20 June 2022
Questions a. All services onboarded through the Engineering and Information Technology function at ICANN org are required to have a Risk Assessment performed and documented. This risk assessment is used for the business to assess the risks of using those external services. Is the intention of the recommendation to introduce the risk assessment requirement for any external party that provides services to ICANN org?
Answer a. A risk assessment is only part of appropriate security governance and management. The implementation shepherds expect ICANN org to create a policy that states what is expected from vendors. A based tiered approach (low, medium, high) for risk, criticality, and sensitivity is one method. Additionally, audit should cover the implementation of the agreed standards including follow up on mitigation measures where gaps are identified, as stated by ICANN's chosen NIST Cybersecurity Framework when it comes to supply chain security:

> "Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations." (ID.SC-4)

ICANN org Assessment:

ICANN org's Engineering & Information Technology (E&IT) function already requires all vendors and service providers to have a risk assessment performed and documented by the Security and Network Engineering Department which meets industry-standard requirements. ICANN org has multiple contracts for vendors. The Board notes that by default such contracts are established with a one-year term. When all active contracts are renegotiated at the end of their term, ICANN org would then be in a position to complete this recommendation.
Proposed Board Action: Approve as fully implemented

SSR2 recommendation	SSR2-defined measures of success	Board Action 22 July 2021
6.1: ICANN org should proactively promote the voluntary adoption of SSR best practices and objectives for vulnerability disclosure by the contracted parties. If voluntary measures prove insufficient to achieve the adoption of such best practices and objectives, ICANN org should implement the best practices and objectives in contracts, agreements, and MOUs**.** **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 6: SSR Vulnerability Disclosure and Transparency (6.1 - 6.2):** This recommendation can be considered implemented when ICANN org promotes the voluntary adoption of SSR best practices for vulnerability disclosures by contracted parties and implements associated vulnerability disclosure reporting. These recommendations can be considered effective when ICANN org and the contracted parties have adopted SSR best practices and objectives for vulnerability disclosure.	The Board notes that several elements of the recommendation are not clear. For example, as written, it is not clear how ICANN org should implement the recommendation in the event that there is not voluntary adoption, and may require a GNSO Policy Development Process. Possibly, the SSR2 Review Team meant "ICANN org should require the implementation of best practices and objectives in contracts, agreements, and Memorandums of Understanding (MOUs)". If this is the intent, while the Board supports contracted parties using best practices that align with the goals and objectives outlined in ICANN's Strategic Plan, making implementation of best practices mandatory would be a policy matter and not something ICANN org or Board can unilaterally impose in "contracts, agreements, and MOUs." Other elements of this recommendation that require clarification include, for example, how should SSR best practices/objectives be identified? How should ICANN org measure adoption? What is the threshold to evaluate ICANN org's promotional efforts as insufficient? The Board directs the ICANN President and CEO, or his designee(s), to seek clarity from the Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

22 July 2021 Board Rationale:
Recommendations 6.1 and 6.2 pertain to SSR vulnerability disclosures, including imposing additional requirements on contracted parties. The community inputs that the Board considered when acting on Recommendations 6.1 and 6.2 showed that while several commenters support the recommendations, others express concerns. RySG, Namecheap, and RrSG believe elements of the recommendations contemplate that ICANN org should unilaterally make modifications to the Registrar Accreditation Agreement (RAA). For example:

- RySG - "While the RySG supports its members adopting vulnerability disclosure policies as good business practice, it does not support ICANN acting as a clearinghouse, gatekeeper, or regulator of vulnerability disclosure policies
- Namecheap - "Namecheap does not support any of the components of the SSR2 Final Report that contemplate any modification of the RAA (including but not limited to Recommendations 6 and 8), and urges the ICANN Board to completely reject any of these recommendations."
- RrSG - "It is not the role of ICANN or the ICANN community to dictate the operational obligations of contractual parties especially without the participation, agreement, and approval of the contracted parties."

While IPC is supportive of these recommendations, IPC expresses a concern that "requir[ing] dotBrands to disclose all vulnerabilities in their business to ICANN...goes beyond ICANN's remit. At a minimum, any vulnerabilities should be limited only to those systems directly related to the operation of the TLD."

With regard to Recommendation 6.1, the Board notes that several elements of the recommendation are not clear. For example, as written, it is not clear how ICANN org should implement the recommendation in the event that there is not voluntary adoption, and may require a GNSO Policy Development Process. Possibly, the SSR2 Review Team meant "ICANN org should require the implementation of best practices and objectives in contracts, agreements, and Memorandums of Understanding". If this is the intent, while the Board supports contracted parties using best practices that align with the goals and objectives outlined in ICANN's Strategic Plan, making implementation of best practices mandatory would be a policy matter and not something ICANN org or Board can unilaterally impose in "contracts, agreements, and MOUs." Other elements of this recommendation that require clarification include, for example, how should SSR best practices/objectives be identified? How should ICANN org measure adoption? What is the threshold to evaluate ICANN org's promotional efforts as insufficient? The Board directs the ICANN President and CEO, or his designee(s), to seek clarity from the Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

With regard to Recommendation 6.2, the Board notes there are three components of this recommendation, which each have different considerations. While ICANN org already does some of the things called for within the recommendation as ICANN org noted in its comments on the SSR2 Review Team draft report, the recommendation's focus on disclosure appears difficult or nearly impossible to implement. The Board directs the ICANN President and CEO, or his designee(s), to consult with the SSR2 Implementation Shepherds to better understand the SSR2 Review Team's intent of the recommendation and the possible process to implement it with the relevant parties. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

SSR2 Implementation Shepherds' responses to clarifying questions were received on 16 March 2022.

"Question a: Is it the intent of SSR2 RT that ICANN org develop these resources for voluntary adoption or make use of already developed resources? If the latter, can the Implementation Shepherds provide references to those resources?

Answer a: As described at the beginning of Section 3 in the SSR2 Final Report, some ccTLDs are certified in accordance to ISO/IEC 27001:2013 and/or ISO 22301:2012. The idea is to encourage gTLDs to follow this example. The ccTLD that have chosen to this approach have resources, and the SSR2 RT did not envision the development of additional resources.

Question b: How should adoption of the voluntary measures be measured?

Answer b: The SSR2 RT is calling for transparency and accountability in this recommendation (and many others). The SSR2 Implementation Shepherds encourage ICANN org to setup a web page that contains the audit status information for TLDs so that registrants can be informed.

Question c: Who should determine whether the voluntary measures are sufficiently or insufficiently adopted?

Answer c: The SSR2 RT recommended standardized audits so that anyone can determine whether the voluntary measures have been adopted. The following web page provides an example, while recognizing that it is not totally on point: https://www.denic.de/en/content-pool/information-security-master/

Question d: Assuming the statement 'ICANN org should implement the best practices and objectives in contracts, agreements, and MOUs' should be interpreted to read 'ICANN org should require contracted parties to implement the best practices and objectives via contracts, agreements, and MOUs', is it the intent of the SSR2 RT for ICANN org to modify existing contracts, agreements, and MOUs to require this implementation or is the intent that future contracts, agreements, and MOUs include this requirement?

Answer d: While the SSR2 RT would prefer the earliest possible adoption, it is well understood that it will take time to work with all of the contracted parties, and some of them will resist change to their agreements. The recommendation is intended for these contracts to be strengthened based on the best practices and incorporated on each re-negotiated agreement or new negotiated."

ICANN org Assessment:
Recognizing that the promotion of SSR best practices in the domain space is appropriate and a task ICANN org already takes on, notably through initiatives such as Knowledge-sharing and Instantiating Norms for DNS and Naming Security (KINDNS), clarification received from SSR2 Implementation Shepherds suggests safeguarding adherence to ISO standards, which is not what the language of the recommendation states. The Board cannot unilaterally impose such a requirement on the business practices of each registry.

In the event adoptions would be "voluntary," additional resources (time or personnel) from ICANN Compliance and other teams would be required to measure and ensure compliance with these. ICANN org will continue to operate under the intent of this recommendation through continued promotion of initiatives that support and encourage voluntary adherence to current BCPs, but does not believe that it can implement this recommendation in a reasonable fashion without significant efforts in the case of "resistant" TLDs, or contract amendments.

ICANN org Proposed Board Action: Reject

SSR2 Recommendation	SSR2-defined measures of success	Board Action 22 July 2021

6.2: ICANN org should implement coordinated vulnerability disclosure reporting. Disclosures and information regarding SSR-related issues, such as breaches at any contracted party and in cases of critical vulnerabilities discovered and reported to ICANN org, should be communicated promptly to trusted and relevant parties (e.g., those affected or required to fix the given issue). ICANN org should regularly report on vulnerabilities (at least annually), including anonymized metrics and using responsible disclosure. **SSR2 designated priority:** High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 6: SSR Vulnerability Disclosure and Transparency (6.1 - 6.2):** This recommendation can be considered implemented when ICANN org promotes the voluntary adoption of SSR best practices for vulnerability disclosures by contracted parties and implements associated vulnerability disclosure reporting. These recommendations can be considered effective when ICANN org and the contracted parties have adopted SSR best practices and objectives for vulnerability disclosure.	The Board notes that several elements of the recommendation are not clear. For example, as written, it is not clear how ICANN org should implement the recommendation in the event that there is not voluntary adoption, and may require a GNSO Policy Development Process. Possibly, the SSR2 Review Team meant "ICANN org should require the implementation of best practices and objectives in contracts, agreements, and Memorandums of Understanding (MOUs)". If this is the intent, while the Board supports contracted parties using best practices that align with the goals and objectives outlined in ICANN's Strategic Plan, making implementation of best practices mandatory would be a policy matter and not something ICANN org or Board can unilaterally impose in "contracts, agreements, and MOUs." Other elements of this recommendation that require clarification include, for example, how should SSR best practices/objectives be identified? How should ICANN org measure adoption? What is the threshold to evaluate ICANN org's promotional efforts as insufficient? The Board directs the ICANN President and CEO, or his designee(s), to seek clarity from the Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

22 July 2021 Board Rationale:
Recommendations 6.1 and 6.2 pertain to SSR vulnerability disclosures, including imposing additional requirements on contracted parties. The community inputs that the Board considered when acting on Recommendations 6.1 and 6.2 showed that while several commenters support the recommendations, others express concerns. RySG, Namecheap, and RrSG believe elements of the recommendations contemplate that ICANN org should unilaterally make modifications to the Registrar Accreditation Agreement (RAA). For example:

- RySG - "While the RySG supports its members adopting vulnerability disclosure policies as good business practice, it does not support ICANN acting as a clearinghouse, gatekeeper, or regulator of vulnerability disclosure policies
- Namecheap - "Namecheap does not support any of the components of the SSR2 Final Report that contemplate any modification of the RAA (including but not limited to Recommendations 6 and 8), and urges the ICANN Board to completely reject any of these recommendations."
- RrSG - "It is not the role of ICANN or the ICANN community to dictate the operational obligations of contractual parties especially without the participation, agreement, and approval of the contracted parties."

While IPC is supportive of these recommendations, IPC expresses a concern that "requir[ing] dotBrands to disclose all vulnerabilities in their business to ICANN...goes beyond ICANN's remit. At a minimum, any vulnerabilities should be limited only to those systems directly related to the operation of the TLD."

With regard to Recommendation 6.1, the Board notes that several elements of the recommendation are not clear. For example, as written, it is not clear how ICANN org should implement the recommendation in the event that there is not voluntary adoption, and may require a GNSO Policy Development Process. Possibly, the SSR2 Review Team meant "ICANN org should require the implementation of best practices and objectives in contracts, agreements, and Memorandums of Understanding". If this is the intent, while the Board supports contracted parties using best practices that align with the goals and objectives outlined in ICANN's Strategic Plan, making implementation of best practices mandatory would be a policy matter and not something ICANN org or Board can unilaterally impose in "contracts, agreements, and MOUs." Other elements of this recommendation that require clarification include, for example, how should SSR best practices/objectives be identified? How should ICANN org measure adoption? What is the threshold to evaluate ICANN org's promotional efforts as insufficient? The Board directs the ICANN President and CEO, or his designee(s), to seek clarity from the Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

With regard to Recommendation 6.2, the Board notes there are three components of this recommendation, which each have different considerations. While ICANN org already does some of the things called for within the recommendation as ICANN org noted in its comments on the SSR2 Review Team draft report, the recommendation's focus on disclosure appears difficult or nearly impossible to implement. The Board directs the ICANN President and CEO, or his designee(s), to consult with the SSR2 Implementation Shepherds to better understand the SSR2 Review Team's intent of the recommendation and the possible process to implement it with the relevant parties. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

SSR2 Implementation Shepherds' responses to clarifying questions were received on 16 March 2022**.**

"Question a: What specific additional requirements does the SSR2 intend to be imposed regarding coordinated vulnerability disclosure reporting that is not already covered in the existing Coordinated Vulnerability Disclosure Reporting framework?

Answer a: The SSR2 RT heard about people that tried to report something and were redirected and redirected until they just gave up. The goal is to provide a single point of reporting, and it looks like the Coordinated Vulnerability Disclosure Reporting framework is intended to do that. The metric of success should be testimony from users that they were able to easily make vulnerability disclosures.

Question b: Please provide examples of specific outcomes and/or benefits to relevant parties the SSR2 RT would expect.

Answer b: Success is achieved when users have an easier time with coordinated vulnerability disclosure reporting.

Question c: Please provide examples of other potential "SSR-related issues" besides breach that should be included in such reporting to ICANN, in accordance with the SSR2 RT's expectations for implementation of this recommendation.

Answer: c: *Please see footnote 29 in the SSR2 Final Report.* The goal is to follow expert guidance regarding breaches and vulnerability disclosures.

Footnote 29 from the SSR2 Final report (page 25): Examples of various ccTLD's that are certified in accordance to ISO/IEC 27001:2013 and/or ISO 22301:2012: DENIC https://www.denic.de/en/content-pool/information-security-master/, IIS https://internetstiftelsen.se/docs/27001-eng-Certificate.pdf , nic.at https://www.nic.at/en/thecompany/certificates-and-awards , Nominet https://www.nominet.uk/security-at-nominet/ ."

ICANN org Assessment:

The SSR2 Implementation Shepherds' response to *Question a* on the Coordinated Vulnerability Disclosure Reporting (CVDR) Framework appears to be anecdotal. Without concrete evidence, there is nothing to suggest that the existing framework is inadequate. ICANN org handles any incidents via an existing process, maintains an incident log, shares vulnerabilities as required. In regard to disclosure reporting, as noted in ICANN org comments on the SSR2 Draft Report:

- "Any disclosures we make in terms of an incident is based on ICANN org's own incident reporting process. ICANN org maintains the Cybersecurity Incident Log at https://www.icann.org/cybersecurityincidentlog. In general, ICANN org will disclose major security vulnerabilities and resulting incidents that cause significant risk to the security of ICANN's systems, or to the rights and interests of data subjects, or otherwise require disclosure under applicable legal requirements. ICANN org's coordinated vulnerability disclosure process is available at https://www.icann.org/vulnerabilities."

As it relates to a process for disclosures and information regarding SSR-related issues, such as "breaches at any contracted party" and reporting to "trusted and relevant parties," these would require modifications to contracted party agreements.

ICANN org Proposed Board Action: Reject

SSR2 Recommendation	SSR2-defined measures of success	22 July 2021 Board action
7.1: ICANN org should establish a Business Continuity Plan for all the systems owned by or under the ICANN org purview, based on ISO 22301 "Business Continuity Management," identifying acceptable BC and DR timelines. **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures (7.1 - 7.5):** This recommendation can be considered implemented when ICANN org's BC and DR plans and processes are thoroughly documented according to accepted industry standards, including regular audits that those	**Board Action on 7.4:** The Board does not have enough information to consider resource implications of implementing this recommendation versus the expected benefit. The Board notes that in its comment on the SSR2 Review Team draft report, ICANN org asked the SSR2 Review Team to provide clear justification as to why it believes the benefits of a third disaster recovery site justifies the costs of such a site. While the recommendation

7.2: ICANN org should ensure that the DR plan for Public Technical Identifiers (PTI) operations (i.e., IANA functions) includes all relevant systems that contribute to the security and stability of the DNS and also includes Root Zone Management and is in line with ISO 27031. ICANN org should develop this plan in close cooperation with the Root Server System Advisory Committee (RSSAC) and the Root Server Operators (RSO). **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org	processes are being followed, and when a non-U.S., non-North American site is operational. This recommendation can be considered effective when ICANN org can demonstrate how they can handle incidents that impact the whole U.S. or North America.	states that the new site could replace "either the Los Angeles or Culpeper sites", the requested cost/benefit information is not provided in the SSR2 Review Team Final Report. Further, the Board notes Section 4.2 of the Internet Assigned Numbers Authority (IANA) Naming Function Contract that prohibits IANA operations outside of the United States, and as such, the Board understands that implementation of this recommendation as written is not currently feasible for some portions of the IANA functions. These restrictions could be removed through contract amendments if there were a desire to do so from the ICANN community, which would require community consultation and discussion. The Board directs the ICANN President and CEO, or his designee(s), to consult with the SSR2 Implementation Shepherds to better understand elements of this recommendation that are not feasible as written, or are not clear, including if the SSR2 Review Team
7.3: ICANN org should also establish a DR Plan for all the systems owned by or under the ICANN org purview, again in line with ISO 27031. **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org		
7.4: ICANN org should establish a new site for DR for all the systems owned by or under the ICANN org purview with the goal of replacing either the Los Angeles or Culpeper sites or adding a permanent third site. ICANN org should locate this site outside of the North American region and any United States territories. If ICANN org chooses to replace one of the existing sites, whichever site ICANN org replaces should not be closed until the organization has verified that the new site is fully operational and capable of handling DR of these systems for ICANN org. **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org		**Board Action on 7.1, 7.2, 7.3, 7.5:** The Board notes that the SSR2 Review Team states successful measures of implementation for these recommendations as: "This recommendation can be considered implemented when ICANN org's Business Continuity (BC) and Disaster Recovery (DR) plans and processes are thoroughly documented according to accepted industry standards, including regular audits that those processes are being followed, and when a non-U.S., non-North American site is operational." The Board is placing Recommendation 7.4, which calls for the "non-U.S., non-North American site" into "pending, likely to be rejected unless additional information shows implementation is feasible." As such, the Board directs the ICANN President and CEO, or his designee(s) to seek clarification from the SSR2 Implementation Shepherds as to if implementation of these recommendations can be considered effective in the event that the Board rejects Recommendation 7.4 regarding opening a non-U.S., non-North American site, and that portion of the success measure cannot be achieved. The Board has a concern with accepting recommendations for which implementation can never be deemed successful or effective. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
7.5: ICANN org should publish a summary of their overall BC and DR plans and procedures. Doing so would improve transparency and trustworthiness beyond addressing ICANN org's strategic goals and objectives. ICANN org should engage an external auditor to verify compliance with these BC and DR plans. **SSR2 designated priority:** Medium-High **SSR2 designated owner:** ICANN org		
22 July 2021 Board Rationale for 7.1, 7.2,7.3, 7.4, 7.5:		

Recommendations 7.1, 7.2, 7.3 and 7.5 pertain to business continuity and disaster recovery processes and procedures. The community inputs that the Board considered when acting on Recommendations 7.1, 7.2, 7.3 and 7.5 showed that most commenters are in support of the recommendations, however RySG notes some concerns:

> RySG - "While the RySG supports the principle being highlighted in this set of recommendations, i.e., having a BC and a DR plan, the proposed scope of 'all the systems owned by or under the ICANN org purview' is too broad, contrary to best commercial practice, and thus inappropriate. BC and DR development should be included as part of an overall risk management strategy as highlighted by the Report in recommendation 4 and elsewhere in existing policies and processes. Similar, for example, to the IANA risk management strategy for its services. We recommend that the Board seek additional clarity from the SSR2 RT regarding how Recommendation 7.2 feeds into the current Governance Working Group developing a governance structure for Root Zone Operators."

The Board notes that the SSR2 Review Team states successful measures of implementation for these recommendations as: "This recommendation can be considered implemented when ICANN org's BC and DR plans and processes are thoroughly documented according to accepted industry standards, including regular audits that those processes are being followed, and when a non-U.S., nonNorth American site is operational." [1] The Board is placing Recommendation 7.4, which calls for the "non-U.S., non-North American site" into "pending, likely to be rejected unless additional information shows implementation is feasible."

As such, the Board directs the ICANN President and CEO, or his designee(s) to seek clarification from the SSR2 Implementation Shepherds as to if implementation of these recommendations can be considered effective in the event that the Board rejects Recommendation 7.4 regarding opening a non-U.S., non-North American site, and that portion of the success measure cannot be achieved. The Board has a concern with accepting recommendations for which implementation can never be deemed successful or effective.

The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

SSR2 Implementation Shepherd responses to clarifying questions were received on 16 March 2022.

7.4

"Question a: What would the Implementation Shepherds consider would be the likelihood of an incident that impacts the whole of the United States or NorthAmerica?

Answer a: The SSR2 Implementation Shepherds recognize that this recommendation might have been more clear had it appeared in the DNSSEC portion of the report. The point of the recommendation is to provide diversity in the jurisdiction in which the facilities that house the DNSSEC Root KSK, even if the facility outside the United States is only for DR purposes.

Question b: The recommendation mentions Culpeper. Culpeper is only used as a KSK facility. ICANN has 2 KSK facilities; Culpeper and El Segundo. ICANN has corporate data center locations elsewhere in DC and LA separate from KSK facilities. Does this recommendation mean the locations where the corporate infrastructure is located? Or the separate locations that house the KSK/IANA infrastructure?

Answer b: This recommendation is about the facilities that house the DNSSEC Root KSK.

Question c. The majority of ICANN org corporate services (payroll, finance, DMS, CMS, email, meeting services, etc.) are provided by third parties. Given that the majority of these outsourced services make up the backbone of business operations for ICANN org, can the implementation shepherds please clarify why having an additional DR site outside of U.S. territory provides enough of an added benefit to justify the additional cost?

Answer c: The point of the recommendation is to provide diversity in the jurisdiction in which the facilities that house the DNSSEC Root KSK. The SSR2 RT felt that this diversity is worth the additional cost."

SSR2 Implementation Shepherd responses to clarifying questions were received on 20 June 2022

"Question a. Would the SSR2 Implementation Shepherds consider 7.1, 7.2, 7.3, 7.5 to be successfully implemented and effective in the event that the Board rejects Recommendation 7.4 regarding opening a non-U.S., non-North American site, and that portion of the success measure cannot be achieved?

Answer a. Not fully, but they would be partially implemented.

7.1

Question a. ICANN org reading of this recommendation is that the SSR2 RT has conflated the goal of Business Continuity Management for the whole of ICANN org, such as what ISO 22301 calls for, with the goals of operational plans for systems disaster recovery to support operational business continuity. In light of ICANN org's interpretation, can the implementation shepherds please clarify the intent of this recommendation?

Answer a. As indicated by the section heading, the goal is BOTH Business Continuity and Disaster Recovery.

7.2

Questions a. The recommendation states "... includes all relevant systems that contribute to the security and stability of the DNS". Since ICANN does not own/operate all of the systems that contribute to the security and stability of the DNS, can the Implementation Shepherds confirm that the scope of this recommendation is meant to only cover systems owned and operated by ICANN org?

[1] SSR2 Review Team Final Report (p30): https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21- en.pdf

Answer a. Correct, this recommendations is aimed at the systems owned and operated by ICANN org. The SSR2 RT is asking ICANN org to lead by example!
Question b. This recommendation calls for a DR plan that is in line with ISO 27031 but ICANN org is seeking clarification to this approach in recommendations 7.1 and 7.3. Once the clarifying questions are answered and a decision is made regarding adopting ISO 27031, do the Implementation Shepherds find it acceptable for this recommendation to follow the same approach?
Answer b. The implementation shepherds understand that ICANN will use the NIST Cybersecurity Framework, and the implementation shepherds think this is a reasonable alternative as long as the implementation is transparent to the community, and is regularly audited and attested by a third party. NIST provides a number of resources regarding audit: **https://www.nist.gov/cyberframework/assessment-auditing-resources [nist.gov]**
7.3
Question a. The recommendation specifies ISO 27031. ICANN org has already commenced adoption and implementation of applicable NIST standards. Would the Implementation Shepherds consider if other standards such as NIST SP 800-34 Rev 1 would meet the requirements of the recommendation?
Answer a. The implementation shepherds understand that ICANN will use the NIST Cybersecurity Framework, and the implementation shepherds think this well accepted standard a reasonable way forward as long as the implementation is transparent to the community so that there is an opportunity to identify and remedy gaps. Regular external, attested audits of the implementation of framework and the resulting controls is most critical for establishing a constantly evolving security program and stature."
7.5
Question a. The recommendation proposes publishing information that is potentially confidential or may lead to exposure of sensitive operational details. Would the Implementation Shepherds accept this item fulfilled if the ICANN Org provided such reports to the ICANN Board?
Answer a. The SSR2 RT used the word "summary" so that the information could be provided at a level that avoids exposure of sensitive operational details.
Question b. The recommendation proposes that the ICANN Org use a 3rd party auditor to review the BC and DR plans to some level of "compliance", can the Implementation Shepherds provide insight on the expected cadence of such audits that would meet the Implementation Shepherd's view as sufficient?
Answer b. Such audits are common practice. The implementation shepherds would expect to see regular audits as part of routine audits performed at ICANN Org internally and by third-party, independent auditors, as is common practice. The sufficient cadence depends on the results of the previous audit and the associated remedies, if any are needed."

ICANN org Assessment:

The SSR2 Implementation Shepherds clarified the intent of Recommendation 7.4 was for having a key management facility outside of the US, solely for the purpose of diversity of jurisdiction. Their clarification seems to be inconsistent with the metrics for success "will be effective when ICANN org can demonstrate how they can handle incidents that impact the whole U.S. or North America".

Additionally, the SSR2 Implementation Shepherds also stated that this facility could be limited solely for disaster recovery. However, the metric states that the recommendation can be considered effective "when a non-U.S., non-North American site is operational." The word *operational* is not defined, but it could be perceived that it requires an ongoing active capability in-line with the existing U.S.-based facilities. If a DR site was to be operationally capable on an ongoing basis, or reasonably instantiated on short notice, a preliminary assessment indicates that it would need to be provisioned and maintained to a level comparable to the currently active sites located within the U.S. If diversity in jurisdiction is the only reason for this facility to be built, it could be worth reviewing more precisely what benefits and risks increased jurisdictional diversity provide, and whether the existing key management processes could be evolved to address possible gaps. While the current two facilities are in the same national jurisdiction, they are geographically diverse and have different local jurisdictions with different regulatory approaches.

The IANA functions themselves, that operate the Root Zone KSK, are conducted by a U.S. organization and would continue to be subject to U.S. legal obligations. The overall design of KSK operations and oversight cover many provisions for diversity of oversight, including various roles for trusted community representatives from around the world.

The Board should also consider the following efforts to decide whether building a non-U.S. facility is the right solution:

- Financial: A facility of this nature is expected to be a considerable investment. In addition to a sizeable upfront cost of construction and commissioning a site, there will be material costs associated with the ongoing maintenance needs to ensure the site is operative (if it were to be an active site), and/or regularly tested and primed for operation (if it were limited for disaster recovery purposes).
- Compliance: This conflicts with key outcomes of the IANA stewardship transition process, which resulted in contractual requirements that the IANA functions can only be conducted within the U.S. The IANA Naming Contract states:
  Section 4.2 U.S. Presence.
  - *(a) Contractor shall be a wholly U.S. owned and operated corporation operating in one of the 50 states of the United States or District of Columbia; (ii) incorporated within the state of California, United States of America; and (iii) organized under the nonprofit public benefit corporation laws of the state of California.*

- *(b) Contractor shall perform the IANA Naming Function in the United States and possess and maintain, throughout the performance of this Contract, a physical address within the United States. Contractor must be able to demonstrate that all primary operations and systems will remain within the United States (including the District of Columbia). ICANN reserves the right to inspect the premises, systems, and processes of all security and operational components used for the performance of the IANA Naming Function.*

- Operational: If there was a contractual ability for these functions to be housed outside the U.S., maintaining an operational site would significantly reshape IANA's staffing requirements and other internal procedures. Either the U.S.-based staff would need to engage in a significant program of ongoing international travel to build and maintain these facilities, or non-U.S. based staff would need to be recruited and maintained to support these operations. It is important to note that the successful operation of the existing U.S.-based facilities is heavily dependent on borrowing personnel from other ICANN org departments to augment IANA staff for ceremony and maintenance operations. For a transnational approach, those support operations would likewise need to be expanded.

Recognizing that management of the DNSSEC Root KSK is part of the IANA functions, an evaluation of existing contractual agreements between ICANN, its affiliate PTI, and the community was conducted. The evaluation showed that the request is likely incompatible with key requirements for the IANA functions under the current contractual language, which derives from outcomes of the multistakeholder IANA stewardship transition process. Of particular note is Section 4.2 of the IANA Naming Functions contract, which states that ICANN, through its affiliate, *"shall perform the IANA Naming Function in the United States and possess and maintain, throughout the performance of this Contract, a physical address within the United States. Contractor must be able to demonstrate that all primary operations and systems will remain within the United States (including the District of Columbia)".*

ICANN org Proposed Board Action: Approve Recommendations 7.1, 7.2, 7.3, 7.5 and reject Recommendation 7.4

SSR2 Recommendation	SSR2-defined measures of success	Board Action 22 July 2021
11.1: The ICANN community and ICANN org should take steps to ensure that access to CZDS data is available, in a timely manner and without unnecessary hurdles to requesters, e.g., lack of auto-renewal of access credentials. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN community and ICANN org	**SSR2-defined measures of success for Recommendation 11: Resolve CZDS Data Access Problems (11.1):** This recommendation can be considered implemented when ICANN org and the community makes access to CZDS data available in a timely manner and without unnecessary hurdles to requesters. This recommendation can be considered effective when ICANN org reports a decrease in the number of zone file access complaints and improves the ability for researchers to study the security-related operations of the DNS.	The Board notes that some elements of this recommendation are not clear. For example, the Board notes that ICANN org is currently in the process of implementing recommendations from SAC097, which calls for ICANN org to revise "the [Centralized Zone Data Service] CZDS system to address the problem of subscriptions terminating automatically by default, for example by allowing subscriptions to automatically renew by default." It is not clear what additional work is needed to sufficiently implement the SSR2 Review Team's Recommendation 11.1 or how the existing work already being performed on CZDS access is insufficient. The Board directs the ICANN President and CEO, or his designee(s) to seek clarity from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

22 July 2021 Board Rationale:
Recommendation 11.1 pertains to the availability of Centralized Zone Data Service (CZDS) data. The community inputs that the Board considered when acting on this recommendation showed that while some community groups are in support of the recommendation, others express concerns. For example:

- RySG - "The current CZDS system not only provides sufficient access but was also the result of lengthy negotiations taking into account the varying needs of different members of the ICANN community, including the registries that provide this access."
- NCSG - "Brand protection and intellectual property protection are not security and stability issues. But in this section 'brand protection' is again invoked. This is a risky path to take and can lead to extending the ICANN mission and the definition of DNS abuse."

The Board notes that some elements of this recommendation are not clear. For example, the Board notes that ICANN org is currently in the process of implementing recommendations from SAC097, which calls for ICANN org to revise "the CZDS system to address the problem of subscriptions terminating automatically by default, for example by allowing subscriptions to automatically renew by default." It is not clear what additional work is needed to sufficiently implement the SSR2 Review Team's Recommendation 11.1 or how the existing work already being performed on

CZDS access is insufficient. The Board directs the ICANN President and CEO, or his designee(s) to seek clarity from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps

SSR2 Implementation Shepherds' responses to clarifying questions were received on 20 June 2022

Question a. ICANN org notes that this recommendation appears to relate to and be in support of SAC097. As the Board notes in the rationale for actions taken on Recommendation 11.1, ICANN org is currently in the process of implementing recommendations from SAC097, which calls for ICANN org to revise "the [Centralized Zone Data Service] CZDS system to address the problem of subscriptions terminating automatically by default, for example by allowing subscriptions to automatically renew by default." ICANN org has provided the Board information regarding a plan to approach and accomplish the recommendations in SAC097. ICANN org also provides quarterly updates on the status of implementation via the Action Request Register. Please confirm the correctness of our understanding that this recommendation is in support of SAC097.

Answer a. The SSR2 report points to the overlap with SAC097. Please keep in mind that SSR2 RT was concerned about the large number of unaddressed CZDS-related complaints, and the SSR2 RT metric of effectiveness is that these complaints stop because CZDS users are satisfied with the CZDS service. To that end, the SSR2 RT wants to ensure that access to CZDS data is available even if all of SAC097 is not implemented by the ICANN Board.

ICANN org Assessment:

Progress of related work and Board Advice:

The status of SAC097 Rec 1, as reported on the public Board Advice page (https://features.icann.org/board-advice) to the SSAC, is as follows:

- "The CZDS 3.0 project will address the SAC097 recommendations related to CZDS including support for zone file access extension prior to their expiration date, automatic renewal of access as the default system behavior, and automatic compliance escalation of unattended access requests in pending status. ICANN org plans to release this new functionality to CZDS in phases.
- The ICANN org continues work on the CZDS 3.0 project, the following milestones have been completed:
  - On 25-April-2022 the CZDS system was updated to offer requestors the option to cancel their pending requests if desired, which is a functionality the community had asked for.
  - On 24-May-2022 infrastructure updates were deployed to the CZDS system to improve performance and service availability for users downloading gTLD zone files.
  - On 28-June-2022 support was added in the CZDS system to allow zone file access requestors to submit an access extension request prior to expiration of their current access, which makes it possible for users to retain uninterrupted access to already authorized zone files as long as the registry operator approves such requests prior to expiration. Optional email notifications for registry operators were also improved to provide a summary of received requests in a single daily digest as opposed to individual notifications.
- Future project milestones still in development include functionality to support automatic renewal of zone file access as the default system behavior, and automatic compliance escalation of unattended access requests in pending status."
- From the public update provided to the SSAC on the status of SAC097 Rec 2 (https://features.icann.org/board-advice):
  - "ICANN org, through the Policy Support team, continues to inform the community to have the recommendation considered for the subsequent rounds of new gTLDs.
  - Once the described functional updates that resulted from Recommendation 1 are applied to the CZDS system, any TLDs added to the CZDS system in the future would be able to offer the same approval policies to end-users.
  - Once the CZDS 3.0 project is complete, the CZDS system will support the same functionality as well as any future zone file access approval policies for any TLD.
  - Functionality already implemented as part of the CZDS 3.0 project will continue to be supported for any TLD added to the system in future rounds."
- From the public update provided to the SSAC on the status of SAC097 Rec 3 (https://features.icann.org/board-advice):
  - "The number of complaints requiring ICANN org's Contractual Compliance follow-up is decreasing. The adoption rate of the new auto-approve feature increased to 45% from 40% in June 2019. The number of TLDs that approve requests for a period longer than 2 years is increasing. SAC097 was prepared in the first half of 2017. Since then ICANN org has worked with registry operators to decrease the number of zone file related complaints by creating awareness about zone files access. This includes multiple engagements and presentations to the gTLD Registries Stakeholder Group, the Brand Registry Group, and individual registries.
- ICANN org's Contractual Compliance is currently training additional staff members to assist in processing complaints related to zone file access requests, allowing for new complaints to be addressed consistently on a timely basis. ICANN org's Contractual Compliance continues to address the contractual scope of denials and revocation of access to zone files with registry operators that appear to misunderstand the boundaries within which registry operators are allowed to do so.
- Additionally, ICANN org's Contractual Compliance has initiated outreach efforts with contracted parties to resolve processing concerns. The total volume of complaints received has remained consistently lower than the total received in June 2021, which was the highest volume received between June 2021 and May 2022.

- ICANN org's Contractual Compliance reiterates that successful implementation of the CZDS 3.0 project should help reduce the number of complaints, as it will, among other things support zone file access extension prior to their expiration date, automatic renewal of access as the default system behavior, and automatic compliance escalation of unattended access requests in pending status."
- From the public update provided to the SSAC on the status of SAC097 Rec 4 (https://features.icann.org/board-advice)
  - "In the past five years since SAC097 was published, the number of gTLDs that inaccurately report zfa-passwords field was reduced by almost 2/3 (June 2017: 45% to May 2022:14%), resulting with 86% of gTLDs reporting this field accurately. Every month, the exact number of zone file access provided (zfa-passwords) are available on CZDS Reports (https://czds.icann.org/reports) publicly for all gTLDs, as required by SAC097.
  - ICANN org published the Registry Monthly Reporting FAQs document (https://www.icann.org/en/system/files/files/registry-monthly-reporting-faqs-31mar22-en.pdff) in June 2022 to provide answers to the common questions and concerns that were received during ICANN org's outreach. This new document will be a continuous support for the registry operators and their technical service providers to generate and submit all reports accurately, despite cases such as turnover volume increases. The conversations between SSAC and registry operators clarified that ICANN org cannot measure the accuracy of the web-based WHOIS query statistics. Therefore, it is not possible for ICANN org to compare the past and current status of the issue by itself. ICANN org is looking forward to supporting the SSAC leadership in their work with the TechOps group, which brings registry operators and their technical service providers together."

- The primary concern of the SSR2 Review Team appears to be a perceived difficulty to access CZDS data when needed, citing the overall number of ZFA complaints and issues such as a "lack of auto-renewal" for CZDS credentials. As noted in the Board action on this recommendation, the implementation of SAC097 should meet the intent of this recommendation and resolve the SSR2 Review Team's concerns. ICANN org notes that the SSR2 Implementation Shepherds acknowledged the work in progress related to SAC097 but also reiterated its concerns regarding CZDS access, regardless of whether SAC097 is implemented.
- ICANN org has conducted considerable work related to the CZDS both since the publication of SAC097 and the SSR2 produced its Final Report. As ICANN org noted in updates to the SSAC (see full updates and download report here), the number of complaints related to ZFA requiring Contractual Compliance follow-up is decreasing. Since the publication of SAC097, ICANN org has worked with registry operators to decrease the number of zone file related complaints by creating awareness about zone files access. This included engagement and multiple presentations to the gTLD Registries Stakeholder Group, the Brand Registry Group, and individual registries. ICANN org's Contractual Compliance continues to address the contractual scope of denials and revocation of access to zone files with registry operators that appear to misunderstand the boundaries within which registry operators are allowed to do so. ICANN org's Contractual Compliance has also dedicated additional members to processing complaints regarding zone file access requests and continues to train new members to assist in processing, thereby amplifying the ability to address new complaints consistently on a timely basis. Since June 2021, the total volume of complaints received has remained consistently lower than the total received in June 2021, which was the highest volume received between June 2021 and May 2022.
- Finally, ICANN org notes that work related to CZDS 3.0 will also play a large role in improving access and alleviating concerns noted by the SSR2 Review Team. Successful implementation of the CZDS 3.0 project should help reduce the number of complaints, as it will, among other things, support zone file access extension prior to their expiration date, automatic renewal of access as the default system behavior, and automatic compliance escalation of unattended access requests in pending status.
- ICANN org notes the latest milestones related to CZDS 3.0:
  - As of 25-April-2022, the CZDS system offers requestors the option to cancel their pending requests if desired, which is a functionality the community had asked for.
  - As of 24-May-2022, infrastructure updates were deployed to the CZDS system to improve performance and service availability for users downloading gTLD zone files.
  - As of 28-June-2022, support was added in the CZDS system to allow zone file access requestors to submit an access extension request prior to expiration of their current access, which makes it possible for users to retain uninterrupted access to already authorized zone files as long as the registry operator approves such requests prior to expiration. Optional email notifications for registry operators were also improved to provide a summary of received requests in a single daily digest as opposed to individual notifications.
- ICANN org also notes a contradiction between the success measures defined in the SSR2 Final Report and the SSR2 Implementation Shepherds' response above. The success measure states that "[t]his recommendation can be considered effective when ICANN org reports a decrease in the number of zone file access complaints". However, the SSR2 Implementation Shepherds' response indicates that "the SSR2 RT metric of effectiveness is that these complaints stop because CZDS users are satisfied with the CZDS service." ICANN org notes that it is likely not possible for "complaints to stop," but ICANN org's Contractual Compliance has already reported a decrease in complaints.

Proposed Board Action: Approve as fully implemented

SSR2 Recommendation	SSR2-defined measures of success	Board Action 22 July 2021

16.2: ICANN org should create specialized groups within the contract compliance function that understand privacy requirements and principles (such as collection limitation, data qualification, purpose specification, and security safeguards for disclosure) and that can facilitate law enforcement needs under the RDS framework as that framework is amended and adopted by the community (see also SSR2 Recommendation 11: Resolve CZDS Data Access Problems). **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org **16.3:** ICANN org should conduct periodic audits of adherence to privacy policies implemented by registrars to ensure that they have procedures in place to address privacy breaches. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org	**SR2-defined measures of success for Recommendation 16: Privacy Requirements and RDS (16.1 - 16.3):** This recommendation can be considered implemented when ICANN org's actions regarding privacy and their management of the RDS are properly documented, and specifically assigned resources within ICANN org keep the organization in line with current best practices and legal requirements in this space. This recommendation can be considered effective when ICANN org can demonstrate ongoing compliance with best practices and legal requirements in data handling and privacy.	**Board Action on 16.2:** The Board is not clear as to what is meant by "facilitate law enforcement needs" and how that is relevant to the role of ICANN org's Contractual Compliance team. As written, ICANN org does not have the authority to do this. Further, the intent of the recommendation is not clear, specifically why the SSR2 Review Team understands the existing subject matter experts and Chief Data Protection Officer roles within ICANN org are inadequate to achieve the requirements of this recommendation. The Board understands that ICANN org's Contractual Compliance team has subject matter experts in the areas listed to the extent that they are necessary for contract enforcement. For other matters and as necessary, ICANN org's Contractual Compliance members can refer to ICANN org's Chief Data Protection Officer for guidance regarding the specific areas listed. Through the Contractual Compliance team, ICANN org enforces policies that have been adopted by the community and makes operational and structural changes as needed to carry out its enforcement role. The Board directs the ICANN President and CEO, or his designee(s), to consult with SSR2 Implementation Shepherds to better understand how the SSR2 Review Team anticipated that ICANN org's Contractual Compliance team can perform the requested actions, as well as other elements of the recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps. **Board Action on 16.3:** The Board noted in its comment on the SSR2 Review Team draft report, ICANN org does not specifically require registrars to have "privacy policies." ICANN org's Contractual Compliance team cannot audit something that is not an ICANN contractual requirement. The Board directs the ICANN President and CEO, or his designee(s) to consult with SSR2 Implementation Shepherds to better understand the SSR2 Review Team's intent of the recommendation. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.
22 July 2021 Board Rationale: Recommendations 16.2 and 16.3 relate to privacy requirements around the Registration Directory Service (RDS). The community inputs that the Board considered when acting on Recommendations 16.2 and 16.3 showed that while several community groups support the recommendations, RySG and RrSG express some concerns that these recommendations do not address a specific problem statement. Concerns in particular with regard to recommendation 16.3 include, for example: - RySG - "16.3 suggests that ICANN Compliance should audit Registry and Registrar compliance with a Registry or Registrar's own internal policies and procedures as opposed to its contractual obligations with ICANN. Such a recommendation exceeds the scope of ICANN Compliance's role to enforce contractual requirements."		

- RrSG - "This is outside of ICANN's scope. ICANN is not a DPA, and the audit would need to cover a number of countries and jurisdictions around the world, and it is unclear how ICANN has the expertise or resources to conduct such an audit."

With regard to Recommendation 16.2, the Board is not clear as to what is meant by "facilitate law enforcement needs" and how that is relevant to the role of ICANN org's Contractual Compliance team. As written, ICANN org does not have the authority to do this. Further, the intent of the recommendation is not clear, specifically why the SSR2 Review Team understands the existing subject matter experts and Chief Data Protection Officer roles within ICANN org are inadequate to achieve the requirements of this recommendation. The Board understands that ICANN org's Contractual Compliance team has subject matter experts in the areas listed to the extent that they are necessary for contract enforcement. For other matters and as necessary, ICANN org's Contractual Compliance members can refer to ICANN org's Chief Data Protection Officer for guidance regarding the specific areas listed. Through the Contractual Compliance team, ICANN org enforces policies that have been adopted by the community and makes operational and structural changes as needed to carry out its enforcement role.

The Board directs the ICANN President and CEO, or his designee(s), to consult with SSR2 Implementation Shepherds to better understand how the SSR2 Review Team anticipated that ICANN org's Contractual Compliance team can perform the requested actions, as well as other elements of the recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

Further, with regard to Recommendation 16.3 which recommends for ICANN org to "conduct periodic audits of adherence to privacy policies implemented by registrars to ensure that they have procedures in place to address privacy breaches"; as the Board noted in its comment on the SSR2 Review Team draft report, ICANN org does not specifically require registrars to have "privacy policies." ICANN org's Contractual Compliance team cannot audit something that is not an ICANN contractual requirement. The Board directs the ICANN President and CEO, or his designee(s) to consult with SSR2 Implementation Shepherds to better understand the SSR2 Review Team's intent of the recommendation. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

SSR2 Implementation Shepherds' responses to clarifying questions were received on 16 March 2022**.**
16.2
"Question a: Please clarify the purpose the RT identified for the creation of specialised groups within Compliance that understands privacy requirements and principles?
Answer a: In the SSR2 Final Report, the three paragraphs before SSR2 Recommendation 16 explain the purpose for the three recommendations in this section. In fact, the last paragraph repeats a request by the RDS review team that was not implemented.
Question b: What kind of role would these groups play? Is the RT suggesting that these new groups should be responsible for enforcement of non-ICANN mandated policies that Contracted Parties might choose to apply to their operations?
Answer b: The role of these groups would be to implement SSR2 Recommendations 16.1, 16.2, and 16.3. They would not be responsible for enforcing registry and registrar policies, but they can track them. For example, ICANN org could require registries and registrars to provide a link to their privacy policies, and then ICANN org can automate publishing the the policies in the online index of registrars. More importantly, this group ought to provide legal expertise and support for law enforcement and consumer protection representatives during evolution of the RDS framework.
Question c. Please describe any current deficiencies the RT identified in enforcement of the RA/RAA privacy requirements.
Answer c: The SSR2 Implementation Shepherds believe facilitate law enforcement and consumer protection needs under the RDS framework while preserving privacy to the greatest extent possible."

16.3
"Question a: Please explain how the SSR2 Implementation Shepherds believe ICANN Compliance can perform audits of privacy policies adopted by registrars outside the requirements of the RAA and community-developed policy, including the authority it believes Compliance has to carry out these actions.
Answers a: The SSR2 Final Report asks the registrars to have procedures in place to address privacy breaches. The SSR2 RT did not ask for an audit that these procedures are followed. Under GDPR, CCPA, and other emerging privacy regulation, the SSR2 Implementation Shepherds think that the procedures should be publicly available. This aspect of transparency is likely to be required regardless of any action taken by ICANN at this point."

ICANN org Assessment:
SSR2 Implementation Shepherds' answers indicate that new groups of ICANN staff within the Contractual Compliance team could track and publish registrars data privacy policies and procedures. ICANN org contracts do not specifically require registrars to have "privacy policies." Tracking suggested in Recommendation 16.2 would be outside the scope of ICANN and its contractual agreements with registries and registrars.

ICANN org's Contractual Compliance team cannot audit privacy policies that are not an ICANN contractual requirement.

Proposed Board Action: Reject.

SSR2 Recommendation	SSR2-defined measures of success	Board Action 22 July 2021
18.1: ICANN org should track developments in the peer-reviewed research community, focusing on networking and security research conferences, including at least ACM CCS, ACM Internet Measurement Conference, Usenix Security, CCR, SIGCOMM, IEEE Symposium on Security and Privacy, as well as the operational security conferences and FIRST, and publish a report for the ICANN community summarizing implications of publications that are relevant to ICANN org or contracted party behavior. **SSR2 designated priority:** Low **SSR2 designated owner:** ICANN org **18.2:** ICANN org should ensure that these reports include relevant observations that may pertain to recommendations for actions, including changes to contracts with registries and registrars, that could mitigate, prevent, or remedy SSR harms to consumers and infrastructure identified in the peer reviewed literature. **SSR2 designated priority:** Low **SSR2 designated owner:** ICANN org **18.3:** ICANN org should ensure that these reports also include recommendations for additional studies to confirm peer-reviewed findings, a description of what data would be required by the community to execute additional studies, and how ICANN org can offer to help broker access to such data, e.g., via the CZDS. **SSR2 designated priority:** Low **SSR2 designated owner:** ICANN org	**SSR2-defined measures of success for Recommendation 18: Informing Policy Debates (18.1 - 18.3)**: This recommendation can be considered implemented when ICANN org creates and maintains a public archive of digests or readouts from various networking and security research conferences. This recommendation can be considered effective when the information coming from the research community on SSR related issues is more accessible to people who are making policy decisions.	While the Board agrees that there is merit to ICANN org performing an evaluation to ensure that it is tracking at an appropriate level to the work that ICANN does, the Board notes that many academic papers published do not reach the level of notice that would impact the work of ICANN and a significant investment of time, money, and effort would be required to sort through these materials. In this manner, Recommendations 18.1 - 18.3 imply unbounded work. The Board would like to better understand the community's views as to if ICANN org should expend additional resources on this activity, in light of current existing work. The Board directs the ICANN President and CEO, or his designee(s), to perform an evaluation of its tracking efforts already underway and provide this to the Board to ensure that ICANN org is tracking at an appropriate level to the work that ICANN does. Further, the Board directs the ICANN President and CEO, or his designee(s) to engage the community to understand if ICANN org should expend additional resources on this activity, in light of current existing work. This information will inform the Board's decision on next steps.

22 July 2021 Board Rationale:

Recommendations 18.1, 18.2 and 18.3 recommend that ICANN org create and maintain a public archive of digests or readouts from various networking and security research conferences. The community inputs that the Board considered when acting on these recommendations showed that while several community groups support these recommendations by way of their overarching support for all recommendations in the SSR2 Review Team Final Report, RySG and RrSG express concerns. For example:

- RySG - "In much the same way that ICANN monitors and offers neutral summary reports on legislative developments and identifier technology issues, it is reasonable for ICANN to do so for other topics related specifically to ICANN's mission and scope. However, it is unclear how recommending that ICANN offer an interpretation or analysis (including proposing additional studies) of these third-party efforts by specifically targeting only one part of the ICANN community is within either the Review Team's scope of work or ICANN's."
- RrSG - "Contract negotiations are between contracted parties and ICANN as detailed in the RAA and RA, and are not subject to public discussion and feedback from the ICANN community, including recommendations from

peer-reviewed literature", and "it is not clear how the studies will be paid for, and how confirming peer-reviewed studies are beneficial or within ICANN's remit."

The Board notes that ICANN org currently already publishes reports of emerging technologies that are relevant to ICANN org's mission through its Office of the Chief Technology Officer (OCTO) publication series, and regularly provides updates the community, for example via recent Emerging Identifier Technology sessions at ICANN58, ICANN60, ICANN64, and ICANN66.

As the Board noted in its comment on the SSR2 Review Team draft report, the Board supports the work of OCTO and its determination of the needs for data and analysis to inform its work, and the Board is not clear about the value to the community of a potentially large-scale and costly effort associated with the implementation of this recommendation. While the Board agrees that there is merit to ICANN org performing an evaluation to ensure that it is tracking at an appropriate level to the work that ICANN does, the Board notes that many academic papers published do not reach the level of notice that would impact the work of ICANN and a significant investment of time, money, and effort would be required to sort through these materials. In this manner, Recommendations 18.1 - 18.3 imply unbounded work. The Board would like to better understand the community's views as to if ICANN org should expend additional resources on this activity, in light of current existing work.

The Board directs the ICANN President and CEO, or his designee(s), to perform an evaluation of its tracking efforts already underway and provide this to the Board to ensure that ICANN org is tracking at an appropriate level to the work that ICANN does. Further, the Board directs the ICANN President and CEO, or his designee(s) to engage the community to understand if ICANN org should expend additional resources on this activity, in light of current existing work. This information will inform the Board's decision on next steps.

ICANN org Assessment:

18.1

- Much of the peer-reviewed research communities (universities and other research communities) work is on items that are out of ICANN's remit.
- Much of such efforts are conceptual or experimental.
- Many of these research communities are open to all for minimal or no cost. There is no direct benefit to have ICANN org act as a proxy to the community.
- Some community members already participate in these (and other) groups and have historically raised awareness of new or emerging concepts and technology at appropriate times
- ICANN org also follows or participates in some of these groups and will raise awareness at appropriate times in the form of presentations, OCTO publications, blogs, internal and board briefings and through other mechanisms
- ICANN org also follows and/or participates in operational forums such as (but not limited to);
    - Internet Engineering Task Force (IETF)
    - Network Operator Groups (NOGs)
    - Network Information Centers (NICs)
    - Registration Operations Workshop (ROW)
    - Other user or operator groups
- When a concept or technology rises beyond conceptual or experimental, and the concept or technology has a potential impact on ICANN org's mission and remit, ICANN org may focus its resources on investigating this technology. ICANN org will use the results of that investigation for internal or board briefings, but may also present, publish, or invite speakers to discuss the technical foundations of this technology. Public proliferation of these findings can be found in forums such as:
    - Formation and launch of Special Interest Forum on Technology (SIFT) - https://www.icann.org/octo/sift-en
    - Emerging Identifier Technology (EIT) sessions at ICANN meetings
        - These presentations are strategically targeted to the relevance of the potential impact of the org and Community
    - OCTO Document Publications - https://www.icann.org/octo/publications
        - These publications try to remain neutral in position and are meant to discuss the technology
    - Investigations of Emerging Identifier Technologies are driven by technologies that could potentially have an impact on ICANN's mission and remit. These technologies may be identified within the standards communities such as; IETF, World Wide Web Consortium (W3C), International Telecommunication Union Standards Sector (ITU-T, etc), through staff or board interest, through community interest, or other means.
    - There are already (mostly) publicly available resources on emerging identifier technology such as (but not limited to);
        - IETF - https://www.ietf.org
        - ITU-T - https://www.itu.int/en/ITU-T/Pages/default.aspx
        - W3C - https://www.w3.org
        - Red Clara - https://www.redclara.net/index.php/en/
        - Network and Distributed System Security (NDSS) Symposium - https://www.ndss-symposium.org
    - Although conceptional technologies may be of interest to some in the community, ICANN org focuses its resources on technologies that are a) implementable and b) have a potential impact on the ICANN ecosystem and/or interest to our broader community stakeholders.
    - These technologies that ICANN org does investigate tend to have a higher probability of impact to the ICANN ecosystem and its stakeholders.

18.2

- 18.2 is dependent on 18.1

- When technical material is produced (through the OCTO Document mechanism), ICANN org makes every effort to keep that technical paper neutral, discussing only the technical merits or deficits of that technology.
- These neutral technical papers or briefings may be used internally or with the board to create an ICANN org position, which will be published, presented, or otherwise proliferated by other means.
- The ICANN Ecosystem has groups in place to also evaluate such emerging technologies such as (but not limited to): Security and Stability Advisory Committee (SSAC), Root Server System Advisory Committee (RSSAC), Public Safety Working Group (PSWG), and SIFT

18.3

- 18.3 is dependent on 18.1
- When ICANN org feels it appropriate, it will either perform or contract additional studies for emerging technology on identifiers.
- This work can take the form of internal studies (fully staff supported), community studies such as the DNS Security Facilitation Initiative (DSFI) or contracted studies, and results of study 1 of the SSAC Name Collision Analysis Project (NCAP) studies.

18.1

ICANN org believes that the level of attention to emerging identifier technologies is appropriate and occurs when any particular technology rises beyond academic or conceptual and into an implementable stage that could have impact on ICANN org's mission or remit. When such a technology does become apparent, ICANN org will investigate and report on the technology in a neutral fashion. ICANN org will then use that investigation to contribute to the organization's position of said technology. These investigations and assessments are not on a regular cadence, but rather, they happen when a new technology rises to a level that could have impact on ICANN org, or the Security, Stability, and Resiliency of the Internet, as decided by the Board, ICANN org executive staff, or from recommendations of our technical teams with the Org.

It is of ICANN org opinion that these investigations are at the appropriate level of attention in which the Org should invest its resources. ICANN org feels that unbound activities such as described in this recommendation would require a significant investment of resources and would only produce minimal, if any, return to the investment that would be beyond the efforts already in place and under way. Therefore, ICANN org recommends that this recommendation be rejected.

18.2 and 18.3

ICANN org believes that the level of attention that it provides is sufficient information at the internal and community level. As noted in 18.1 Summary Assessment, new concepts or technologies that have a direct or probable impact on the identifiers which fall within ICANN org's remit do not happen at a predictable timeframe. When such an event does take place, ICANN org will investigate these new technologies and report to the Board, staff, and community at an appropriate level through the mechanisms described in 18.1.

With reference to this grouping of recommendations in the July 2021 Board ask "to engage the community to understand if ICANN org should expend additional resources on this activity, in light of current existing work", org reviewed community comments received in response to the SSR2 Final Report on this set of recommendations. The org noted that while the first comment, from the Registrar Stakeholder Group, was against implementing such recommendations, the second one from ALAC, suggested ICANN to increase engagement and take an active role. In reviewing the two comments received through the public comment proceeding, and in further assessing the recommendations feasibility and ICANN org's current measures, it was determined that no further engagement would be needed to inform this. ICANN org invites the community to continue to raise awareness regarding emergent technologies perceived to impact ICANN's mission.

Proposed Board Action: Reject

SSR2 Recommendation	SSR2-defined measures of success	Board Action 22 July 2021
20.1: ICANN org should establish a formal procedure, supported by a formal process modeling tool and language to specify the details of future key rollovers, including decision points, exception legs, the full control-flow, etc. Verification of the key rollover process should include posting the programmatic procedure (e.g., program, finite-state machine (FSM)) for public comment, and ICANN org should incorporate	**SSR2-defined measures of success for Recommendation 20: Formal Procedures for Key Rollovers (20.1 - 20.2):** This recommendation can be considered implemented when ICANN org develops formal process and verification that offers verification of the key rollover process after each key rollover, and when ICANN org begins to run regular tabletop	**Board Action on 20.1**: The Board expects that this recommendation would require significant resources to implement, while the cost versus benefit is not clear. Further, the Board notes that this recommendation has dependencies on research work that has not yet been conducted, such as algorithm rolls. The Board notes that alternative solutions, such as a process that contains evaluation checkpoints that allow circumstances to be evaluated and

community feedback. The process should have empirically verifiable acceptance criteria at each stage, which should be fulfilled for the process to continue. This process should be reassessed at least as often as the rollover itself (i.e., the same periodicity) so that ICANN org can use the lessons learned to adjust the process. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org **20.2:** ICANN org should create a group of stakeholders involving relevant personnel (from ICANN org or the community) to periodically run table-top exercises that follow the Root KSK rollover process. **SSR2 designated priority:** Medium **SSR2 designated owner:** ICANN org	exercises to test and familiarize participants with the key rollover process. This recommendation can be considered effective when the SSR of the process by which DNSSEC protections are maintained during root zone KSK key rollovers are formally verifiable.	provide for potential course correction, may be more appropriate. In light of these considerations, the Board requires further information, including from community engagement as appropriate, in order to take dispositive action on this recommendation. The Board directs the ICANN President and CEO, or his designee(s) to gather further information, including via community engagement and engagement with the SSR2 Implementation Shepherds as appropriate on this recommendation. This information will inform the Board's decision on next steps. **Board Action on 20.2:** While the recommendation appears feasible and the Board believes that table-top exercises would be beneficial, more information is needed to understand what the SSR2 Review Team intended to be targeted in the table-top exercises following the Root key signing key (KSK) rollover process. The Board directs the ICANN President and CEO, or his designee(s) to seek clarification from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps and whether Recommendation 20.2 can be approved.

22 July 2021 Board Rationale:
Recommendation 20.1 relates to establishing a formal procedure to specify the details of future key rollovers. No community groups express concerns about this recommendation. The Board expects that this recommendation would require significant resources to implement, while the cost versus benefit is not clear. Further, the Board notes that this recommendation has dependencies on research work that has not yet been conducted, such as algorithm rolls. The Board notes that alternative solutions, such as a process that contains evaluation checkpoints that allow circumstances to be evaluated and provide for potential course correction, may be more appropriate. In light of these considerations, the Board requires further information, including from community engagement as appropriate, in order to take dispositive action on this recommendation.

The Board directs the ICANN President and CEO, or his designee(s) to gather further information, including via community engagement and engagement with the SSR2 Implementation Shepherds as appropriate on this recommendation. This information will inform the Board's decision on next steps.

Recommendation 20.2 calls for ICANN org to "create a group of stakeholders involving relevant personnel (from ICANN org or the community) to periodically run table-top exercises that follow the Root Key Signing Key (KSK) rollover process." While the recommendation appears feasible and the Board believes that table-top exercises would be beneficial, more information is needed to understand what the SSR2 Review Team intended to be targeted in the table-top exercises following the Root KSK rollover process. The Board directs the ICANN President and CEO, or his designee(s) to seek clarification from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps and whether Recommendation 20.2 can be approved.

SSR2 Implementation Shepherds' responses to clarifying questions were received on 16 March 2022**.**
20.1
"Questions a: ICANN org has a small internal team that conducts this type of work and there are also many unknowns about the research level (e.g. what an algorithm roll would entail; whether an 'empirically verifiable' business process is accomplishable). Because of this, ICANN org proposes that it would be more realistic and practical to have a process that contains evaluation checkpoints that allow circumstances to be assessed and provide for a potential course correction. Would the RT find this acceptable?
Answer a: The recommendation is based on research and live clinical results that have already been produced, and an openly available process-definition too (based on a formal language) called Little-JIL. The research that was conducted used this tool and process definition language to model live patient medical processes (i.e., specifying the process that doctors must follow when treating patients to ensure their medical safety). The SSR2 RT felt that this

research would generalize to key transitions in the DNSSEC Root zone, which would likely be far less complex than the medical processes that were modeled and implemented in the research literature. *Please see footnote 117 in the SSR2 Final Report for two references to this research*. Little-JIL uses a graphical interface to construct processes, which is likely to be as helpful to DNSSEC Root key management as it was to doctors and patients in the medical setting."

SSR2 Implementation Shepherds' responses to clarifying questions were received on 10 January 2022**.**
20.2
"Questions: We understand and agree that once Recommendation 20.1 (Formal Procedures for Key Rollovers) is implemented, a tabletop exercise is beneficial. Can the SSR2 Implementation Shepherds clarify some of the targets of this exercise? More specifically:

- i. Would scheduling tabletops to coincide with key rollovers, procedural changes, or other events where the input is considered most valuable be sufficient to meet the "periodic" timeframe recommended by the SSR2?
- ii. For existing tabletop exercises within ICANN, ICANN org identifies those internal departments and external SMEs that are evaluated to be most appropriate to exercise the planned scenarios. In developing a tabletop exercise in response to this recommendation, ICANN org anticipates a similar process, likely involving external stakeholders such as trusted community representatives. Did the SSR2 intend for there to be additional parameters to guide ICANN org's development of these tabletop exercises, and if so, please identify?

This will help the org better estimate the level of effort that would be required, as well as perform a high level cost-benefit analysis of this recommendation.
Answer: Yes, the tabletop exercises should be conducted prior to key rollovers and after procedural changes. These tabletop exercises ensure that all parties are prepared for possible contingencies. In addition, after the first two or three tabletop exercises, subsequent tabletop exercises should be conducted every two or three years to help identify any gaps in the procedures. Consideration for the scenario development can take into account previous events that might impact a seamless rollover and events that may change overall system dependencies or redundancy. We did not have additional parameters in mind. That said, after the first tabletop exercise is conducted, we recommend public consultation, particularly with SSAC, as part of the implementation plan. The consultation will allow the community to suggest improvements for subsequent tabletop exercises."

ICANN org Assessment:
In addressing the request for clarification on 20.1, the SSR2 Implementation Shepherds suggested that ICANN org pursue a novel model that cannot be implemented with existing resources and expertise. The SSR2 Implementation Shepherds cite research done in the medical field and believe it can be replicated in the DNSSEC Root Key Management. In addition to the data being irrelevant to the recommendation, ICANN org is not aware of this approach having been researched or used in fields with direct applicability to its processes. After review and discussion, ICANN org found that it is likely not feasible to realistically divert the small amount of resources available to learn about this methodology, or to devote significant expenditure on hiring experts to develop such a complex and specific model with only speculative outcomes, and no assurance that it would provide improved outcomes over the alternative process ICANN org suggested.

Recommendation 20.2 is dependent on 20.1. As Recommendation 20.1 cannot be implemented, ICANN org will not be able to conduct tabletop exercises that follow that process. ICANN org agrees with the underlying drivers for 20.1 and 20.2, that there is benefit in planning possible outcomes and testing the approaches accordingly, however the specific modelling approach being requested would require significant resources for a speculative theoretical outcome that may not be achievable.

Proposed Board Action: Reject, cannot be approved in whole

SSR2 recommendation	SSR2-defined measures of success	Board Action 22 July 2021
24.1: ICANN org should coordinate end-to-end testing of the full EBERO process at predetermined intervals (at least annually) using a test plan that includes datasets used for testing, progression states, and deadlines, and is coordinated with the ICANN contracted parties in advance to ensure that all exception legs are exercised, and publish the results. **SSR2 designated priority:** Medium	**SSR2-defined measures of success for Recommendation 24: Improve Transparency and End-to-end Testing for the EBERO Process (24.1 - 24.2):** This recommendation can be considered implemented when ICANN org coordinates annual end-to-end testing of the full EBERO process with public documentation for the outcome. This recommendation can be considered effective when ICANN org is able to validate that the	The Board notes that some elements of this recommendation are not clear. For example, it is not clear if the SSR2 Review Team's intent is for ICANN org conduct Emergency Back-end Registry Operator (EBERO) testing on "live" gTLDs with registrations. The Board directs the ICANN President and CEO, or his designee(s) to seek clarity from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2

SSR2 designated owner: ICANN org	EBERO process functions as intended, protecting registrants and providing an additional layer of protection to the DNS.	Implementation Shepherds will inform the Board's decision on next steps.

22 July 2021 Board Rationale:
SSR2 Recommendation 24.1 asks ICANN org to perform annual end-to-end testing of the full EBERO process with public documentation for the outcome. No community groups express concerns about this recommendation. The Board notes that some elements of this recommendation are not clear. For example, it is not clear if the SSR2 Review Team's intent is for ICANN org conduct EBERO testing on "live" gTLDs with registrations. The Board directs the ICANN President and CEO, or his designee(s) to seek clarity from the SSR2 Implementation Shepherds on elements of this recommendation that are not clear, such as those noted above. The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board's decision on next steps.

SSR2 Implementation Shepherds' responses to clarifying questions were received on 20 June 2022
"Question a. Is the SSR2 Review Team's intent for ICANN org to conduct Emergency Back-end Registry Operator (EBERO) testing on "live" gTLDs with registrations?
Answer a. No, EBERO testing on "live" gTLDs is not anticipated."

ICANN org Assessment:

- **The SSR2 Implementation Shepherds indicated that the intent of the recommendation is not to conduct testing on "live" gTLDs**. ICANN org understands this to mean that testing is not expected to be conducted on currently active TLDs with registrations.
- **ICANN org notes that it is still not clear what expectations the SSR2 had in mind for testing to be "coordinated with contracted parties,"** as testing of the EBERO process would not involve a currently active TLD with registrations. Moreover, it is unlikely that a contracted party would be willing or able to participate, as the EBERO process is intended for use in situations where a registry is at risk of failing to sustain any of the five critical registry functions.
- **ICANN org notes that in its agreements with the EBERO service providers, there is a provision which allows for EBERO Readiness Exercises** to be conducted annually. The agreements contain a full test plan and expectations from the EBERO service provider.
- **ICANN org has previously conducted testing on gTLDs that were in the process of terminating their registry agreements**. Although these gTLDs did not have registrants, they could be considered "live". These tests allowed for ICANN to demonstrate the effectiveness and proper functioning of the EBERO process as well as fully review the process for issues and areas for improvement.

Proposed Board Action: Approve as fully implemented