

SSR2 Pending - Further Clarification
Clarifying Questions for Implementation Shepherds
May 2022

On 22 July 2021, the Board took action on the 63 SSR2 recommendations as issued in the [SSR2 Review Team Final Report](#), as noted within the [Scorecard titled "Final SSR2 Review Team Recommendations – Board Action."](#)

The Board directed the ICANN President and CEO, or his designee(s), to provide to the Board relevant information, as requested in the Scorecard, or periodic updates on progress toward gathering relevant information, starting within six months from this Board action, in order to support further Board action on each recommendation. The Board commits to take further action on these recommendations subsequent to the completion of steps as identified in the Scorecard.

This document addresses twelve (12) of the 34 pending recommendations, specifically placed into the category pending, holding to seek clarity or further information. More specifically, they are recommendations 3.1, 3.2, 3.3, 4.3, 5.3, 7.1, 7.2, 7.3, 7.5, 9.3, 11.1, 24.1

We are requesting that the SSR2 Implementation Shepherds respond to the clarifying questions for each of the following recommendations.

For context on each of the recommendations we have provided the seven SSR2 RT Final recommendations with Defined Measures of Success, Board Action and Board Rationale addressing the need for clarifying questions.

Questions directed to the SSR2 Implementation Shepherds are noted below the Board Rationale section for each recommendation.

SSR2 Recommendation	SSR2-Defined Measures of Success	Board Action
Recommendations that the Board determines to be pending, holding to seek clarity or further information		
<p>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.</p> <p>SSR2 designated priority: High</p> <p>SSR2 designated owner: ICANN org</p>	<p>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.</p>	<p>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.</p> <p>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.</p>
<p>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.</p> <p>SSR2 designated priority: High</p> <p>SSR2 designated owner: ICANN Board and ICANN org</p>		
<p>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.</p>		

SSR2 Pending - Further Clarification
Clarifying Questions for Implementation Shepherds
May 2022

SSR2 designated priority: High

SSR2 designated owner: ICANN Board and ICANN org

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.”
- [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.

Questions for Implementation Shepherds:

3.1, 3.2, 3.3, 4.3:

- a. 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](#)?
 (see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management)

3.1:

- b. ICANN org’s current plan for reporting framework and engagement reflects an annual cycle of reporting with 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?

SSR2 Pending - Further Clarification
Clarifying Questions for Implementation Shepherds
May 2022

- 3.2, 3.3:**
- c. 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.
 - i. Do the above mentioned elements generally address the intended purpose of recommendations 3.2 and 3.3?
 - ii. Is there additional work beyond what is already in place to meet the requirements of the recommendation?

SSR2 Recommendation	SSR2-Defined Measures of Success	Board Action
<p>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).</p> <p>SSR2 designated priority: High</p> <p>SSR2 designated owner: ICANN org</p>	<p>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.</p>	<p>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.</p> <p>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.</p> <p>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.</p>

SSR2 Pending - Further Clarification
Clarifying Questions for Implementation Shepherds
May 2022

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.

Questions for Implementation Shepherds:

4.3:

- 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?
- 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](#)?
(see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management)

SSR2 Pending - Further Clarification
Clarifying Questions for Implementation Shepherds
May 2022

SSR2 Recommendation	SSR2-Defined Measures of Success	Board Action
<p>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.</p> <p>SSR2 designated priority: High</p> <p>SSR2 designated owner: ICANN org</p>	<p>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.</p>	<p>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.</p>
<p>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.</p>		
<p>Questions for Implementation Shepherds:</p> <p>5.3</p> <p>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?</p>		

SSR2 Recommendation	SSR2-Defined Measures of Success	Board Action
<p>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.</p> <p>SSR2 designated priority: Medium-High</p>	<p>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 processes are being followed, and when a non-U.S., non-North</p>	<p>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</p>

**SSR2 Pending - Further Clarification
Clarifying Questions for Implementation Shepherds
May 2022**

<p>SSR2 designated owner: ICANN org</p> <p>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).</p> <p>SSR2 designated priority: Medium-High</p> <p>SSR2 designated owner: ICANN org</p>	<p>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.</p>	<p>for the “non-U.S., non-North American site” into “pending, likely to be rejected unless additional information shows implementation is feasible.”</p> <p>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.</p> <p>The outcome of the engagement with the SSR2 Implementation Shepherds will inform the Board’s decision on next steps.</p>
<p>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.</p> <p>SSR2 designated priority: Medium-High</p> <p>SSR2 designated owner: ICANN org</p>		
<p>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.</p> <p>SSR2 designated priority: Medium-High</p> <p>SSR2 designated owner: ICANN org</p>		
<p>Board Rationale: 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:</p> <p>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.”</p> <p>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</p>		

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

**SSR2 Pending - Further Clarification
Clarifying Questions for Implementation Shepherds
May 2022**

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.

Questions for Implementation Shepherds:

7x:

- 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?

7.1:

- 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?

7.2:

- 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?
- 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 ISO27031, do the Implementation Shepherds find it acceptable for this recommendation to follow the same approach?

7.3:

- 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?

7.5

- 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 Org provided such reports to the ICANN Board?
- 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.

SSR2 Recommendation	SSR2-Defined Measures of Success	Board Action
<p>9.3: ICANN org should have compliance activities audited externally at least annually and publish the audit reports and ICANN org response to audit recommendations, including implementation plans.</p> <p>SSR2 designated priority: High</p> <p>SSR2 designated owner: ICANN org</p>	<p>SSR2-defined measures of success for Recommendation 9: Monitor and Enforce Compliance (9.1 - 9.4): This recommendation can be considered implemented when audits are happening regularly, and summaries published. This recommendation can be considered effective when ICANN org has completed an audit successfully and reported out to the community.</p>	<p>The Board notes that some elements of this recommendation are not clear, such as what would be audited, against what criteria, by whom, or why an external auditor would be required. The Board directs the ICANN President and CEO, or his designee(s), to seek clarity from the SSR2 Implementation Shepherds on 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.</p>

**SSR2 Pending - Further Clarification
Clarifying Questions for Implementation Shepherds
May 2022**

Board Rationale:

Recommendation 9.3 recommends that ICANN org has “compliance activities audited externally at least annually and publish the audit reports and ICANN org response to audit recommendations, including implementation plans.” The community inputs that the Board considered when acting on Recommendation 9.3 showed that most commenters support the recommendation, although RySG and RrSG note some concerns. For example:

- [RySG](#) - “The implication of Recommendation 9 is that ICANN Compliance is not enforcing the terms of the Registry Agreement or the Registrar Accreditation Agreement. The Registries disagree with this characterization and note that Registry Operators’ compliance with their abuse obligations were recently audited by ICANN Compliance.
- [RrSG](#) - “Any audit of Contractual Compliance should focus on its structure, staffing, activities, systems, processes, and the overall efficiency and effectiveness of this function. Contractual Compliance team already has significant resources within its team and ICANN org to oversee and ensure consistent and accurate complaint processing.”

The Board notes that some elements of this recommendation are not clear, such as what would be audited, against what criteria, by whom, or why an external auditor would be required. The Board directs the ICANN President and CEO, or his designee(s), to seek clarity from the SSR2 Implementation Shepherds on 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.

Questions for Implementation Shepherds:

9:3:

- a. What “Compliance activities” do the SSR2 Implementation Shepherds intend to be audited?
- b. What would be the scope of the audits?
- c. What standards would Compliance be audited against?
- d. What kinds of information would be requested that is not currently already published within the ICANN Contractual Compliance Dashboard <https://features.icann.org/compliance/dashboard/2022/0322/report>, or the ICANN Contractual Compliance Twelve-Month Trends Report: <https://features.icann.org/compliance/dashboard/trends-list?>

SSR2 Recommendation	SSR2-Defined Measures of Success	Board Action
<p>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.</p> <p>SSR2 designated priority: Medium</p> <p>SSR2 designated owner: ICANN community and ICANN org</p>	<p>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.</p>	<p>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.</p>

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.”

SSR2 Pending - Further Clarification
Clarifying Questions for Implementation Shepherds
May 2022

- [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.

Questions for Implementation Shepherds:

11:1:

- 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 (<https://features.icann.org/board-advice/ssac>). Please confirm the correctness of our understanding that this recommendation is in support of SAC097.

SSR2 Recommendation	SSR2-Defined Measures of Success	Board Action
<p>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.</p> <p>SSR2 designated priority: Medium</p> <p>SSR2 designated owner: ICANN org</p>	<p>SSR2-defined measures of success for Recommendation 24: Improve Transparency and End-to-end Testing for the EBERO Process (24.1 - 24.2):</p> <p>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 EBERO process functions as intended, protecting registrants and providing an additional layer of protection to the DNS.</p>	<p>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 Implementation Shepherds will inform the Board’s decision on next steps.</p>

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.

Questions for Implementation Shepherds:

24.1:

- 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?