Source	SSR2 Section or Rec	Report Section	Comment	Response
ICANN Board	0		While in no way criticizing the approach the SSR2 RT took to establish the priorities they assigned, the Board encourages the SSR2 RT to consider relevant factors such as dependencies and relationships with other community work, determination of effort, as compared to expected impact of implementation work, or degree of complexity, among others, in order to categorize each recommendation as 'high priority', 'medium priority', or 'low priority'. This analytical and tiered approach will provide a more useful guideline for planning timely implementation of the recommendations.	The recommendations have been reprioritized. Please see Section B.1. Summary Table and Section B.2. Prioritization.
RrSG	0		It is not clear how the recommendations below will be carried out. While some recommendations are directed to the ICANN Board or ICANN Org (and within their remit, e.g. audit of Compliance or staffing), many of the recommendations would need to to go through the PDP process to avoid having ICANN org creating policy. Those recommendations that include policy elements should be referred to the GNSO Council for further action.	Where appropriate, the review team has highlighted paths to implementation that do not require a PDP. Please see Section E.3. PDP Alternatives.
RySG	0		the proposed recommendations would benefit from an explicit statement of the problem that each over-arching recommendation is intended to address.	The review team has clarified the recommendations to make the problems clearer, and has added a short summary in each family of recommendations to indicate how a future review team will be able to determine if the intended effect of the recommendation was achieved.
ICANN Board	0		Further, the Board notes that it is unclear what information and analysis the SSR2 RT considered when forming its recommendations. These elements of each recommendation should be well understood by all for the Board to properly consider the recommendations and make appropriate instructions to ICANN org and/or community. Section 4.1 of the Operating Standards for Specific Reviews (Operating Standards) provides guidance on how to formulate concrete fact-based problem statements and clear definition of what the desired outcome will look like,including how implementation should be evaluated by the community and the next review team, and the impact of implementation on ICANN resources and on the ICANN community workload.	The review team declines to estimate the resources required to implement these recommendations.
ICANN Board	0		To the extent SSR2 recommendations have dependencies with other multistakeholder processes across ICANN, it is important that the Board maintain and confirm its role, as specified in the Bylaws. Where the SSR2 RT is aware of such overlap, the Board encourages the SSR2 RT to suggest that its recommendations be consolidated into or passed through to ongoing work conducted by the community, or to clarify how the intent of the SSR2 RT's recommendation is to implement something beyond what is already in progress. The Board suggests that clarification regarding the SSR2 RT's expectations for these recommendations may also assist with the SSR2 RT's prioritization efforts, in line with the Board's comment above.	The SSR2 Review Team highlighted such overlap in the text of the recommendations where they could confirm that overlap existed.
BC	1	Complete the implementation of all relevant SSR1 recommendations	The BC believes this is critical. ICANN Org has incorrectly represented these recommendations as implemented, when in fact practically none are completed. These recommendations are nearly eight years old, and the time has long since passed for their implementation.	We believe that a prompt implementation of Suggestion 1 will allow the ICANN community to track the implementation of recommendations of all review teams, not just SSR. The tracking and visibility will allow the ICANN community to raise concerns much earlier in the timeline.
M3AAWG	1	Complete the implementation of all relevant SSR1 recommendations.	(1) Implement SSR1 RT recommendations and other, prior recommendations from ICANN advisory committees, as directed by the ICANN Board.	Thank you.
SSAC	1	Complete the implementation of all relevant SSR1 recommendations.	(3.1.1) It would be helpful for the SSR2 final report to provide a more thorough clarification of the reasons why these SSR1 recommendations are, in SSR2 RT's opinion, not fully implemented.	Appendix D: Findings Related to SSR1 Recommendations describes the gaps found by the SSR2 Review Team and indicates which new SSR2 recommendations address the gaps found in the original recommendations.

Source	SSR2 Section or Rec	Report Section	Comment	Response
SSAC	1	Complete the implementation of all relevant SSR1 recommendations.	(3.1.2) The SSAC has some concerns about the viability of implementation of such a significant list of actions. Specifically, the SSAC is concerned about the extent, cost, sequence, and timeframe of the necessary actions required to implement all of these recommendations. Are there other measures that the SSR2 RT may wish to propose that would give the 135 proposed recommendations a significant prospect of avoiding the same incomplete fate as the 27 outstanding SSR1 recommendations by the time of the next SSR review?	The review team indicates in Section A. Executive Summary that "the detail required to make each recommendation fully SMART, including assigning appropriate timelines, will require thought and action from the implementation team and should be included in the final implementation plan."
NCSG	1	Complete the implementation of all relevant SSR1 recommendations	The NCSG considers of vital importance to implement the recommendations from SSR1 that have not been implemented yet, especially Recommendations 9 and 6. In fact, the team found that 26 SSR1 recommendations were not completely implemented and 2 haven't been implemented at all. Therefore, the NCSG invites ICANN board/Org to provide justifications on those matters and take immediate actions to start their implementation in a timely manner. Moreover, the SSR review Team noted that there are four repeating issues (page 22 and 23 of the draft report subjected to this call for Public Comment). We would like to ask ICANN's Board what actions they will be taking in order to prevent such a situation from occurring again in the future. The affected SSR1 recommendations are the numbers #9, #12, #15, #16, #20, #22, #27, they have now been re-addressed in the recommendations 1 to 5 of the SSR2 that were reviewed by the WS1 team.	Thank you.
ICANN Board	1	Complete the implementation of all relevant SSR1 recommendations	To that end the Board encourages the SSR2 RT to provide for each SSR1 recommendation an analysis of why it believes that ICANN org's implementation efforts do not meet the intent of the recommendation, specific details as to what the SSR2 RT sees as the outstanding issues or risks for each SSR1 recommendation, how the SSR2 RT suggests each recommendation should be addressed considering the extensive developments that may have impacted the recommendations issued nearly eight years ago, and what relevant metrics could be applied to assess implementation in the future.	Appendix D: Findings Related to SSR1 Recommendations describes the gaps found by the SSR2 Review Team. Recognizing that many of the SSR1 recommendations were insufficiently specified, the SSR2 Review Team took the approach of incorporating the necessary direction in their own recommendations. The findings for each SSR1 recommendation (see Appendix D) include pointers to the appropriate SSR2 Recommendation that should resolve the open issues of SSR1.
RrSG	1	Complete the implementation of all relevant SSR1 recommendations	The RrSG agrees with this recommendation.	Thank you.
ICANN Org	1	The SSR2 RT strongly recommends that the ICANN Board and ICANN org complete the implementation of the SSR1 Recommendations.	ICANN org encourages the SSR2 RT to provide for each SSR1 recommendation: ● An analysis of why it believes that ICANN org's implementation efforts do not meet the intent of the recommendation. ● Specific details as to what the SSR2 RT sees as the outstanding issues or risks for each SSR1 recommendation. ● Clarification on how the SSR2 RT suggests each recommendation should be addressed considering the extensive developments that may have impacted the recommendations issued nearly eight years ago. ● Relevant metrics that could be applied to assess implementation in the future.	Appendix D: Findings Related to SSR1 Recommendations describes the gaps found by the SSR2 Review Team. Recognizing that many of the SSR1 recommendations were insufficiently specified, the SSR2 Review Team took the approach of incorporating the necessary direction in their own recommendations. The findings for each SSR1 recommendation (see Appendix D) include pointers to the appropriate SSR2 Recommendation that should resolve the open issues of SSR1.
RySG	1	Complete the implementation of all relevant SSR1 recommendations.	Unless indicated elsewhere in our comments, the RySG supports the implementation of all relevant recommendations.	Thank you.

Source	SSR2 Section or Rec	Report Section	Comment	Response
GAC	1	Complete the implementation of all relevant SSR1 recommendations.	the report could provide a more detailed assessment clarifying the reasons why the SSR1 recommendations are deemed to not have been fully implemented. This would be also relevant due to the large number of recommendations especially if take into account both the SSR1 and SSR2 recommendations (combined, they amount to 53 main recommendations and this number is even higher if we take each specific item of the SSR2 report into consideration).	Appendix D: Findings Related to SSR1 Recommendations describes the gaps found by the SSR2 Review Team. Recognizing that many of the SSR1 recommendations were insufficiently specified, the SSR2 Review Team took the approach of incorporating the necessary direction in their own recommendations. The findings for each SSR1 recommendation (see Appendix D) include pointers to the appropriate SSR2 Recommendation that should resolve the open issues of SSR1.
IPC	1		The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below. It is the IPC's position that these outstanding SSR1 recommendations must be implemented and are critical to the effective implementation of any new SSR2 recommendations. As the RT finds 27 of the initial 28 recommendations to still be relevant, the IPC strongly supports the recommendation that all relevant SSR1 recommendations be expeditiously implemented.	Thank you.
SSAC	1		(3.1.3) The SSAC believes that with so many recommendations from both reports where there appears to be overlap or adjacency between recommendations in SSR1 and SSR2 that they should group them accordingly, ensure that they are in fact distinct recommendations and not duplicates, and that the proposed actions and deliverables are unique. A table and categories for each class of recommendations in the reports would likely serve both the RT and the audience well.	The SSR2 Review Team has merged several related recommendations. Please see Section B.1. Summary Table for the list of recommendations clearly organized into specific groupings.
BC	2	SSR1 Recommendation 9 - Information Security ManagementSystems and Security Certifications	The BC concurs with this recommendation.	Thank you.
SSAC	2	SSR1 Recommendation 9 - Information Security Management Systems and Security Certifications	(3.1.3) Given that Recommendation 1 of the SSR2 report recommends the completion of the SSR1 recommendations, and Appendix D of the SSR2 report contains further details relating to findings and conclusions, including SSR1 Recommendation 9, SSR2 Recommendation 2 seems duplicative.	The SSR2 Review Team noted that many of the SSR1 Recommendations were not fully implemented, often due to a lack of specificity in the original recommendations. The review team feels that a re-evaluation of the original recommendations is still in order, but included specific guidance in the SSR2 recommendations themselves. Please see SSR2 Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications for more information specifically around the need to implement an ISMS.
NCSG	2	SSR1 Recommendation 9 - Information Security Management Systems and Security Certifications	#Recommendation 2 requires ICANN to conduct periodic reviews, audits, etc. of their system's security, stability, and resiliency. We would like to suggest that the review team proposes a specific cycle to conduct the checks. The NCSG suggests that they are conducted on a yearly basis.	The SSR2 Review Team indicated that actual timing should be coordinated with the implementation team and included in the final implementation plan. See Section A. Executive Summary.
RrSG	2	SSR1 Recommendation 9 - Information Security Management Systems and Security Certifications	It makes sense for ICANN Org to be certified for key critical certifications like ISO 27001 and 27701. Such certifications will advance ICANN Org as an organization in terms of data protection and system security. Contracted parties will also benefit if ICANN ORG has certification like ISO 27001 and 27701 regarding their accountability towards compliance with laws or if they use such certifications themselves. ICANN Org management, the CEO, and the ICANN Board most fully support such certifications. The ICANN Board should adopt an accountability oversight mechanism for the Board members.	Thank you. Please see SSR2 Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications for updated text to this recommendation.

Source	SSR2 Section or Rec	Report Section	Comment	Response
ICANN Org	2	SSR1 Recommendation 9 - Information Security Management Systems and Security Certifications	ICANN org considers this recommendation to already be implemented and asks the SSR2 RT to clarify the observed issue or risk, clearly identify a desired outcome and describe how success will be measured. (See supporting detail in the public comment report)	The SSR2 Review Team noted that many of the SSR1 Recommendations were not fully implemented, often due to a lack of specificity in the original recommendations. The review team feels that a re-evaluation of the original recommendations is still in order, but included specific guidance in the SSR2 recommendations themselves. Please see SSR2 Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications for the newly clarified text.
RySG	2		The RySG supports this recommendation.	Thank you. Please see SSR2 Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications for updated text to this recommendation.
IPC	2		The IPC is supportive of this recommendation.	Thank you. Please see SSR2 Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications for updated text to this recommendation.
BC	3	SSR1 Recommendations 12,15, and 16 - SSR Strategy and Framework, Metrics, and Vulnerability Disclosures	The BC concurs with this recommendation.	Thank you. Please see SSR2 Recommendation 6: SSR Vulnerability Disclosure and Transparency for updated text to this recommendation.
SSAC	3	SSR1 Recommendations 12,15, and 16 - SSR Strategy and Framework, Metrics, and Vulnerability Disclosures	(3.1.4) Given that Recommendation 1 of the SSR2 report recommends the completion of the SSR1 recommendations, and Appendix D of the SSR2 report contains further details relating to findings and conclusions, including SSR1 Recommendations 12, 15, and 16, SSR2 Recommendation 3 seems duplicative.	The SSR2 Review Team noted that many of the SSR1 Recommendations were not fully implemented, often due to a lack of specificity in the original recommendations. The review team feels that a re-evaluation of the original recommendations is still in order, but included specific guidance in the SSR2 recommendations themselves. Please see SSR2 Recommendation 6: SSR Vulnerability Disclosure and Transparency for the newly clarified text.
NCSG	3	SSR1 Recommendations 12,15, and 16 - SSR Strategy and Framework, Metrics, and Vulnerability Disclosures	#Recommendation 3 requires ICANN to elaborate the framework and agree with the Metrics and Vulnerability Disclosure. We believe that this process should be done in collaboration with the community represented through the SGs.	The revised recommendation notes that adoption is voluntary and that discussion with the community will likely result in greater adoption. Please see SSR2 Recommendation 6: SSR Vulnerability Disclosure and Transparency for the newly clarified text.
RrSG	3	SSR1 Recommendations 12,15, and 16 - SSR Strategy and Framework, Metrics, and Vulnerability Disclosures	The RrSG doubts that such methods can be applied on a global level without discriminating against certain regions and/or creating high costs for specific contracted parties in certain areas. Modification of the contracts and agreements should not go through a consensus document process. The output from such consensus documents can be considered during arrangements negotiations like any other discussion points during such negotiations.	The SSR2 Review Team removed the community consensus requirement of the recommendation. Please see SSR2 Recommendation 6: SSR Vulnerability Disclosure and Transparency for the newly clarified text.
RySG	3	SSR1 Recommendations 12,15, and 16 - SSR Strategy and Framework, Metrics, and Vulnerability Disclosures	The RySG generally supports this recommendation. However, the RySG notes that contract changes can be triggered only by Consensus Policy or contract negotiations. Further, the RySG suggests that the recommendation clarify that the vulnerability disclosure reporting is for the ICANN organization and that ICANN is not a general clearinghouse for vulnerability reports for all contracted parties - those should be directed to the relevant party.	The SSR2 Review Team has significantly revised this recommendation. Please see SSR2 Recommendation 6: SSR Vulnerability Disclosure and Transparency for the newly clarified text.
IPC	3		The IPC is supportive of this recommendation.	Thank you. Please see SSR2 Recommendation 6: SSR Vulnerability Disclosure and Transparency for updated text to this recommendation.

Source	SSR2 Section or Rec	Report Section	Comment	Response
SSAC	3.1	ICANN org should address security issues clearly, publicly (with consideration for operational security, e. g., after an established moratorium and anonymization of the information, if required), and promote security best practices across all contracted parties.	(3.1.5) This recommendation prompted several questions from the SSAC: How does this differ from current ICANN org procedures? What factors led the SSR2 RT to reach this conclusion? Is there an inference that ICANN org has not addressed security issues? The second part of the recommendation relating to promoting security best practices appears to be a distinct issue and merits further clarification. Is ICANN org deficient in this area, and does the SSR2 RT propose actions that would implement their recommendation? Specifically, where are the gaps in capabilities and actions by ICANN org or community in this area? What specific best practices does the SSR2 RT believe should be developed or implemented to address such gaps, and what do they envision as a useful framework to catalog, share, and enhance operational best practices related to a given topic that is relevant to the ICANN community?	The SSR2 Review Team has significantly revised this recommendation. Please see SSR2 Recommendation 6: SSR Vulnerability Disclosure and Transparency for the newly clarified text.
SSAC	3.2	ICANN org should also capture SSR-related best practices in a consensus document, establish clear, measurable, and trackable objectives, and then implement the practices in contracts, agreements, and MOUs	(3.1.6) The SSAC believes that this recommendation is not practical and cannot be implemented in a reasonable time frame. ... There is a definite need to consider new security-related policies that could become binding for ICANN's contracted parties, but the proposed process using a consensus approach drawn from a very broad community of diverse interests does not appear to be an optimal solution.	The SSR2 Review Team has significantly revised this recommendation. Please see SSR2 Recommendation 6: SSR Vulnerability Disclosure and Transparency for the newly clarified text.
ICANN Org	3.2	SSR Recommendation 3.2: "SSR-related best practices"	Requests for clarification of terms	Please see the revised language in SSR2 Recommendation 6.1., which states "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. "
SSAC	3.3	ICANN org should implement coordinated vulnerability disclosure reporting. Disclosures and information regarding SSR-related issues should be communicated promptly to trusted, relevant parties (e.g., those affected or required to fix the given issue), such as in cases of breaches at any contracted party and in cases of key vulnerabilities discovered and reported to ICANN org.	(3.1.7) The actions in this recommendation are unclear. SSAC understands that ICANN org has, appropriately, already implemented responsible disclosure on a need-to-know basis. What is ICANN org not doing at present that it should do? How does one measure whether the reporting is done appropriately or not when such disclosures cannot necessarily be open disclosures?	Clarification regarding this item may be found in Section D.3. Risk and Security Management, in particular "ICANN org manages a critical system with global impact and should provide security-relevant information and associated data to the community."

Source	SSR2 Section or Rec	Report Section	Comment	Response
SSAC	3.4	ICANN org should establish a clear communication plan for reports to the community and produce regular (at least annual) and timely reports containing anonymous metrics of the vulnerability disclosure process. These communiques should contain responsible disclosure as defined by the community-agreed process and include anonymized metrics.	(3.1.8) SSAC understands that ICANN org has established a vulnerability disclosure process. What aspects of this recommendation differ from ICANN org's current practices?	The SSR2 Review Team is referring to vulnerabilities beyond those in solely ICANN-operated systems. The goal is to have greater transparency in the reporting of vulnerabilities. Please see SSR2 Recommendation 6.2 for revised text.
ICANN Org	3.4	ICANN org should establish a clear communication plan for reports to the community and produce regular (at least annual) and timely reports containing anonymous metrics of the vulnerability disclosure process. These communiques should contain responsible disclosure as defined by the community-agreed process and include anonymized metrics.	ICANN org asks the SSR2 RT to clarify which "community-agreed process" this recommendation refers to. ... If the SSR2 RT believes additional improvements are needed, ICANN org asks that the SSR2 RT identify what gaps exist that the Cybersecurity Incident Log does not address.	The SSR2 Review Team has taken this comment into consideration and the rewritten recommendation specifies the qualities the review team would like to see. Please see SSR2 Recommendation 6.2.
BC	4	SSR1 Recommendation 20 and 22 - Budget Transparency and Budgeting SSR in new gTLDs	The BC concurs with this recommendation. Budget transparency would provide a clear indicator of ICANNOrg's prioritization of SSR-related recommendations.However, the BC disagrees with the concept that ICANN may be less transparent according to level of effort involved, as a subjective determination--ICANN must strive for transparency throughout each of its processes.	Thank you.This recommendation has been clarified in SSR2 Recommendation 3: Improve SSR-Related Budget Transparency.
SSAC	4	SSR1 Recommendation 20 and 22 - Budget Transparency and Budgeting SSR in new gTLDs	(3.1.9) Given that Recommendation 1 of the SSR2 report recommends the completion of the SSR1 recommendations, and Appendix D of the SSR2 report contains further details relating to findings and conclusions, including SSR1 Recommendations 20 and 22, SSR2 Recommendation 4 appears duplicative. Please see the SSAC's feedback in 3.1.3 regarding the overlap or adjacency between recommendations in SSR1 and SSR2.	Thank you, we addressed this by providing a new structure. The SSR2 Review Team noted that many of the SSR1 Recommendations were not fully implemented, often due to a lack of specificity in the original recommendations. The review team feels that a re-evaluation of the original recommendations is still in order, but included specific guidance in the SSR2 recommendations themselves.

Source	SSR2 Section or Rec	Report Section	Comment	Response
NCSG	4	SSR1 Recommendation 20 and 22 - Budget Transparency and Budgeting SSR in new gTLDs	Recommendation 4 deals with Budget Transparency and Budgeting SSR in the new gTLDs. We suggest that the SSR2 team check how or whether this is related or could be integrated into the ongoing work of the new gTLDs PDP working group.	Thank you. The review team is seeking budget transparency in the entire budget, not just the new gTLD budget. Please see SSR2 Recommendation 3: Improve SSR-Related Budget Transparency for revised text.
RrSG	4	SSR1 Recommendation 20 and 22 - Budget Transparency and Budgeting SSR in new gTLDs	The RrSG supports this recommendation	Thank you.This recommendation has been clarified in SSR2 Recommendation 3: Improve SSR-Related Budget Transparency.
RySG	4	SSR1 Recommendation 20 and 22 - Budget Transparency and Budgeting SSR in new gTLDs	The RySG supports this recommendation.	Thank you.This recommendation has been clarified in SSR2 Recommendation 3: Improve SSR-Related Budget Transparency.
IPC	4		The IPC is supportive of this recommendation. Budget transparency would be helpful in reflecting ICANN's commitment to SSR recommendations, however the opening language of this recommendation (e.g., "Where possible" and "reasonable in terms of effort") leaves open the possibility that ICANN could circumvent the transparency intended by this recommendation.	Thank you.This recommendation has been clarified in SSR2 Recommendation 3: Improve SSR-Related Budget Transparency.
ICANN Org	4.1	Where possible (contractually) and reasonable in terms of effort (i.e., over 10% of the activity described in the budget line item), ICANN should be more transparent with the budget for parts of ICANN org related to implementing the Identifier Systems Security, Stability, and Resiliency (IS-SSR) Framework and performing SSR-related functions, including those associated with the introduction of new gTLDs.	...If the SSR2 RT does not consider the current operational model to meet the requirements of SSR2 recommendation 4.1, ICANN org asks the SSR2 RT to provide details as to how it suggests this recommendation should be addressed considering the developments that have occurred since the SSR1 recommendation issued nearly eight years ago, and what relevant metrics could be applied to assess implementation in the future.	This text has been revised in SSR2 Recommendation 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."
BC	5	SSR1 Recommendation 27 - Risk Management	The BC concurs with this recommendation.	Thank you. Please see SSR2 Recommendation 4: Improve Risk Management Processes and Procedures for updated text to this recommendation.

Source	SSR2 Section or Rec	Report Section	Comment	Response
SSAC	5	SSR1 Recommendation 27 - Risk Management	(3.1.10) Given that Recommendation 1 of the SSR2 report recommends the completion of the SSR1 recommendations, and Appendix D of the SSR2 report contains further details relating to findings and conclusions, including SSR1 Recommendation 27, SSR2 Recommendation 5 appears duplicative. The SSAC is aware that ICANN org maintains a centralized risk matrix. To what extent do the measures proposed in SSR2 Recommendation 5 differ from current practice within ICANN org? What is the failing in the organisation's policies and procedures that motivate this recommendation? Please see the SSAC's feedback in 3.1.3 regarding the overlap or adjacency between recommendations in SSR1 and SSR2.	The SSR2 Review Team believes the main issues in the Risk Management area for ICANN is the need for clearer documentation and auditable process. Please see Section D.3. Risk and Security Management and SSR2 Recommendation 4: Improve Risk Management Processes and Procedures for further clarifications regarding the review teams findings and associated recommendation.
RrSG	5	SSR1 Recommendation 27 - Risk Management	The RrSG supports this recommendation, which should build upon ICANN Org existing risk management structure.	Thank you. The review team has not suggested replacing the risk structure; building on the current environment makes sense. Please see SSR2 Recommendation 4: Improve Risk Management Processes and Procedures for the revised text.
ICANN Org	5	SSR1 Recommendation 27 - Risk Management	ICANN org considers this recommendation already to be implemented and asks the SSR2 RT to clarify the observed issue, clearly identify a desired outcome, and describe how success will be measured.	The SSR2 Review Team believes the main issues in the Risk Management area for ICANN is the need for clearer documentation and auditable process. Please see Section D.3. Risk and Security Management and SSR2 Recommendation 4: Improve Risk Management Processes and Procedures for further clarifications regarding the review teams findings and associated recommendation.
RySG	5		The RySG supports this recommendation and suggests that it is bundled with recommendations 7, 8 and 9.	This recommendation was merged with recommendation 7 to form SSR2 Recommendation 4: Improve Risk Management Processes and Procedures. Recommendations 8 and 9 were merged to form SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures.
IPC	5		The IPC is supportive of this recommendation.	Thank you. Please see SSR2 Recommendation 4: Improve Risk Management Processes and Procedures for updated text to this recommendation.
BC	6	Create a Position Responsible for Both Strategic and Tactical Security and Risk Management	The BC concurs with this recommendation and further recommends this position be installed as an executive at the C-level of ICANN.	Thank you. Please see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management.
SSAC	6	Create a Position Responsible for Both Strategic and Tactical Security and Risk Management	(3.2.1) The SSAC believes that it would be helpful to understand the context of this recommendation in the light of the existing organisational structure and capabilities of ICANN org.	Please see Section D.1. Organization Structure Improvements - C-Suite Security Position for further clarification of this recommendation.
NCSG	6	Create a Position Responsible for Both Strategic and Tactical Security and Risk Management	#Recommendation 6: recommends ICANN to create a C-suite position for Risk Management or within C-Suite for Strategy. We acknowledge that and recommend that the Review team draft a job description that could fit the role. This job description could be appended to the final report.	We feel ICANN org and Board should create this function. There is clear guidance in relevant standards. Reference is made to the inclusion of a reference to NIST 800-53, which describes roles for risk management controls. Please see Section D.1. Organization Structure Improvements - C-Suite Security Position and SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management for additional information.
ICANN Board	6	Create a Position Responsible for Both Strategic and Tactical Security and Risk Management	As noted above, as a general observation on the formulation of draft recommendations, the Board encourages the SSR2 RT to provide specific details as to what issues or risks the SSR2 RT has identified with the current operations, how the SSR2 recommendation will address these issues or risks, and what relevant metrics could be applied to assess implementation.	There is clear guidance in relevant standards regarding the importance of centralizing this role. Reference is made to the inclusion of a reference to NIST 800-53, which describes roles for risk management controls. Please see Section D.1. Organization Structure Improvements - C-Suite Security Position and SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management for additional information.

Source	SSR2 Section or Rec	Report Section	Comment	Response
RrSG	6	Create a Position Responsible for Both Strategic and Tactical Security and Risk Management	The RrSG agrees that there should be a position responsible for strategic and tactical security and risk management; it is not clear why this does not already exist. If the fucntion does not already exist, it seems to be a function that fits within the OCTO remit, and so should be part of that team. The RrSG does not consider this specific recommendation as one that requires a PDP; this is something that ICANN Org and the Board can do directly.	There is clear guidance in relevant standards regarding the importance of centralizing this role. Reference is made to the inclusion of a reference to NIST 800-53, which describes roles for risk management controls. Please see Section D.1. Organization Structure Improvements - C-Suite Security Position and SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management for additional information.
ICANN Org	6	Create a Position Responsible for Both Strategic and Tactical Security and Risk Management	ICANN org encourages the SSR2 RT to provide specific details as to what issues, risks, or gaps the SSR2 RT has identified with the current operations, how the SSR2 recommendation will address these issues, risks, or gaps, and what relevant metrics could be applied to assess implementation.	There is clear guidance in relevant standards regarding the importance of centralizing this role. Reference is made to the inclusion of a reference to NIST 800-53, which describes roles for risk management controls. Please see Section D.1. Organization Structure Improvements - C-Suite Security Position and SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management for additional information.
RySG	6	Create a Position Responsible for Both Strategic and Tactical Security and Risk Management	The RySG does not support this recommendation. We agree that ICANN may not currently have one single-threaded owner for SSR-related work and budgets (though we agree OCTO is performing some of these functions and the Board or Finance are performing others), but we believe this can be accomplished with the resources available. Given there is a distinction between the management of internal ICANN IT systems that seems to be under the purview of ICANN's Chief Information Officer and ICANN's responsibility for the security and stability of the DNS that is the remit of the Chief Technology Officer, perhaps it would be more realistic to recommend more transparency of areas of duplication and clarity as to lines of responsibility.	The SSR2 ReviewTeam notes the concerns raised by RySG and would like to reiterate that while these functions can be found in various existing positions within ICANN org, the SSR2 believes that this function needs to be at a strategic level where the risk controls can be organization-wide.
IPC	6		The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below. The IPC supports the SSR2 RT's recommendation that a C-Suite level executive officer position be created to coordinate and strategically manage ICANN's security and risk management objectives. As the RT points out, the current system that decentralizes the roles related to SSR across two separate units within ICANN appears unlikely to be effective. The IPC agrees with this assessment, particularly in light of ICANN's failure to efficiently implement the SSR1 objectives that have been outstanding since 2012. It is the hope of the IPC that a designated officer, supported by a sufficient budget and staff, will be able to more efficiently prioritize and implement these critical security and risk management activities for which ICANN is responsible. Accordingly, the IPC is strongly supportive of the RT' s recommendations related to this new position, including SSR2 Recommendation 7: "Further Develop a Security Risk Management Framework."	Thank you. Please see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management.
BC	7	Further Develop a Security Risk Management Framework	The BC concurs with this recommendation. In particular, the BC agrees with the recommendation regarding measurement. Too often, ICANN does not benefit from measurement data that could help mitigate abuse, improve processes, inform policymaking, or otherwise assist the community. The BC concurs with the RDS2 RT's previous recommendation that all new policies include tracking metrics to understand the policy's efficacy; measurement of success, therefore,is an important part of the SSR2 RT's recommendation here. ICANN should endeavor to source these metrics internally rather than soliciting less-than-reliable, self-reported information from the community.	Thank you. Please see SSR2 Recommendation 4.2 for the update text for this recommendation.

Source	SSR2 Section or Rec	Report Section	Comment	Response
SSAC	7	Further Develop a Security Risk Management Framework	(3.2.2) This is a restatement of Recommendation 5 and it is unclear what objective is achieved through this repetition. The SSAC comments in relation to Recommendation 5 apply here, including the tensions relating to the levels of open disclosure of risk profiles. An appropriate attitude to risk is that an organisation's activities should be informed by risk, but not necessarily fully dictated by considerations of risk. This is the opposite of the direction espoused by recommendation 7.3.2. The SSAC suggests that the report should clarify what is being requested here and clearly identify how this recommended action and the associated deliverables differ from related recommendations in this report.	The review team has merged the two recommendations mentioned into one, and has noted that any public outputs will require some text to be redacted. Please see SSR2 Recommendation 4: Improve Risk Management Processes and Procedures.
RrSG	7	Further Develop a Security Risk Management Framework	This recommendation seems redundant with recommendation 2. Audits and an ISMS are part of the ISO certification, so this level of detail seems excessive. Everything in this recommendation is something that ICANN should do for recommendation 2.	The team is aware that this is technically required but aims to give some details to staff and community on what we consider the most important aspects. The guidance for the Security Risk Management Framework can now be found in SSR2 Recommendation 4: Improve Risk Management Processes and Procedures, whereas the guidence regarding an ISMS can now be found in SSR2 Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications.
ICANN Org	7	SSR2 Recommendation 7: "security risk management"	Requests for clarification of terms	The text has been clarified. Please see Section D.3. Risk and Security Management and SSR2 Recommendation 4: Improve Risk Management Processes and Procedures.
ICANN Org	7	Further Develop a Security Risk Management Framework	As noted above, ICANN org seeks clarification as to what is meant by "security risk management" as opposed to risk management more generally. The main elements and outcomes of ISO 31000 are included in the ICANN org's risk management framework. Under the framework, ICANN org uses its own in-house resources to achieve the same outcomes in a fit-for-purpose way. In this regard, ICANN org considers parts of this recommendation to be duplicative of SSR2 Recommendation 5.	An external audit provides confidence that everything is being done properly. Please see Section D.3. Risk and Security Management and SSR2 Recommendation 4: Improve Risk Management Processes and Procedures for updated text.
RySG	7		The RySG supports this recommendation and suggests that it is bundled with recommendations 5, 8 and 9.	This recommendation was merged with recommendation 5 to form SSR2 Recommendation 4: Improve Risk Management Processes and Procedures. Recommendations 8 and 9 were merged to form SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures.
IPC	7		The IPC is supportive of this recommendation.	Thank you. Please see SSR2 Recommendation 4: Improve Risk Management Processes and Procedures for updated text.
BC	8	Establish a Business Continuity Plan Based on ISO 22301	The BC concurs with this recommendation.	Thank you. Please see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures for updated text.
RrSG	8	Establish a Business Continuity Plan Based on ISO 22301	With the exception of 8.3, this recommendation seems redundant with recommendation 2, which would require ICANN do to this for ISO certification.	Business Continuity and Disaster Recovery services are critical systems on their own; the SSR2 Review Team believes the specific guidance offered is necessary for ICANN. Please see the revised text of SSR2 Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications and SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures for revised language for these areas.

Source	SSR2 Section or Rec	Report Section	Comment	Response
ICANN Org	8	Establish a Business Continuity Plan Based on ISO 22301	This recommendation mentions Disaster Recovery and Business Continuity Planning. ICANN org considers the recommendation regarding disaster recovery already to be implemented. ICANN org has established disaster recovery and continuity plans for systems for ICANN org and IANA functions. Due to potential risks of providing attackers with information to facilitate attack, documents regarding disaster recovery and continuity planning are confidential. The Board has oversight responsibility for ensuring that these programs are in place. ICANN org supports the recommendation to establish a Continuity Plan for all of ICANN org. Such a Continuity Plan is currently under development as part of the ICANN org's Risk Management Framework.	The SSR2 Review Team did not find information on ICANN org's BC/DR plans more recent than 2017. Best practice is to review and revise these plans annually. Please review the SSR2 Review Team's findings in Section D.4. Business Continuity Management and Disaster Recovery Planning, and the clarified language in SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures.
RySG	8	Establish a Business Continuity Plan Based on ISO 22301	The RySG supports this recommendation and suggests that it is bundled with recommendations 5, 7 and 9.	This recommendation was merged with recommendation 9 to form SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures. Recommendations 5 and 7 were merged to form SSR2 Recommendation 4: Improve Risk Management Processes and Procedures.
IPC	8		The IPC is supportive of this recommendation.	Thank you. Please see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures for updated text.
RrSG	8.3	For Public Technical Identifiers (PTI) operations (IANA functions, including all relevant systems that contribute to the Security and Stability of the DNS and also Root Zone Management), ICANN org should develop a shared approach to service continuity in close cooperation with the Root Server System Advisory Committee (RSSAC) and the root server operators	The RrSG supports recommendation 8.3.	Thank you. Please see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures for updated text.
BC	9	Ensure the Disaster Recovery Plan is Appropriate, Functional, and Well Documented	In general, the BC supports Recommendation 9. However, we suggest ICANN should develop and manage an ISO 22301 Business Continuity Management Systems (BCMS), which clearly indicate regular testing of disaster recovery sites and publishing test results within a specified period to all stakeholders as required. The BC also suggests regular internal auditing to prepare adequately for external audits and certification. We also recommend that the implementation team undergo individual certification in ISO 22301/ISO 27031 Implementation and Lead Auditor (I & L.A) program to prepare them in the efficient implementation of Business Continuity Plan (BCP).	Thank you. Please see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures for updated text.
RrSG	9	Ensure the Disaster Recovery Plan is Appropriate, Functional, and Well Documented	This recommendation seems redundant with recommendation 2, which would require ICANN do to this for ISO certification.	Business Continuity and Disaster Recovery services are critical systems on their own; the SSR2 Review Team believes the specific guidance offered is necessary for ICANN. Please see the revised text of SSR2 Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications and SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures for revised language for these areas.

Source	SSR2 Section or Rec	Report Section	Comment	Response
ICANN Org	9	Ensure the Disaster Recovery Plan is Appropriate, Functional, and Well Documented	As noted with regard to SSR2 Recommendation 8, ICANN org considers this recommendation already to be implemented. Further, ICANN org encourages the SSR2 RT to include a clear justification as to why it believes the benefits of a third disaster recovery site justifies the costs of such a site.	The SSR2 Review Team has added language to the findings and recommendation regarding the need for a third DR site. Please review the SSR2 Review Team's findings in Section D.4. Business Continuity Management and Disaster Recovery Planning, and the clarified language in SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures.
RySG	9	Ensure the Disaster Recovery Plan is Appropriate, Functional, and Well Documented	The RySG supports this recommendation and suggests that it is bundled with recommendations 5, 7 and 8.	This recommendation was merged with recommendation 8 to form SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures. Recommendations 5 and 7 were merged to form SSR2 Recommendation 4: Improve Risk Management Processes and Procedures.
IPC	9		The IPC is supportive of this recommendation.	Thank you. Please see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures for updated text.
BC	10	Improve the Framework to Define and Measure Registrar & Registry Compliance	The BC concurs with this recommendation and encourages both staff and the Board to take active roles in their implementation. ICANN's compliance function needs improvement, both in the manner in which it is staffed and in the tools it has available to correct problematic behavior on the part of contracted parties or their customers.This recommendation, correctly implemented, would have a lasting impact on ICANN Org's capability to address abuse and ensure security and resilience.The BC further agrees with the specific recommendation about bringing the EPDP to a close and implementing WHOIS policy. All parties need and deserve the predictability that will come with a fully implemented policy.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
SSAC	10	Improve the Framework to Define and Measure Registrar & Registry Compliance	(3.3.2) Unless the underlying contractual commitments exist to compel contracted parties to act within clearly defined parameters and responsibilities, then the compliance measures proposed here seem ineffectual. Does the SSR2 RT believe that these contracts are sufficiently prescriptive with respect to behaviours and the residual issue is simply one of enforcement of compliance? As the report notes, "Compliance has few options to enforce the agreements" and the measurements proposed in this recommendation appear to 5 measure ineffectuality of enforcement. Are there measures that could have a beneficial outcome on improving this space?	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
NCSG	10	Improve the Framework to Define and Measure Registrar & Registry Compliance	#Recommendation 10: The SSR2 team justifies, elaborates more, analyzes impact and compares what they are recommending here to the current modes of operations. We also note that the recommendation strays into suggesting board action on areas which the review team is not empowered to comment on such as current GNSO policymaking.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
RrSG	10	Improve the Framework to Define and Measure Registrar & Registry Compliance	In general, this recommendation is for policy and should go through the ICANN policy process. Regarding the sub recommendations:	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
RySG	10	Improve the Framework to Define and Measure Registrar & Registry Compliance	The RySG notes that Compliance's size and scope has grown exponentially in recent years and we disagree with SSR2's characterization and implication that contractual compliance is so under-enforced or under-resourced that entire new teams need to be hired to deal with specific issues. We note this throughout the report, but call it out specifically here.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.

Source	SSR2 Section or Rec	Report Section	Comment	Response
IPC	10		The IPC is generally supportive of this recommendation, and discusses its support for this recommendation in greater detail below. The RT recommends, and the IPC supports, several methods for ICANN to better utilize its relationships with the Registrars and Registries to combat DNS abuse, including SSR2 Recommendation 10: “Improve the Framework to Define and Measure Registrar & Registry Compliance,” SSR2 Recommendation 15: “Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse,” and SSR2 Recommendation 16: “Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats.” The IPC supports these recommendations and any steps to more effectively combat DNS abuse relating to the Registry Agreement (RA) and Registrar Accreditation Agreement (RAA) contracts. ... Accordingly, the IPC supports these SSR2 recommendations that would require meaningful enforcement of existing obligations of registries and registrars to prohibit certain security threats and abusive activities, enhance such requirements to further mitigate such activities, include real consequences for registrants who engage in prohibited abusive behavior, and motivate active and consistent investigation and response to reports of abuse by registrars.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
ICANN Board	10.1	Establish a performance metrics framework to guide the level of compliance by Registrars and Registries for WHOIS obligations (including inaccuracy), as well as other elements that affect abuse, security, and resilience, as outlined in the RDS/WHOIS2 Review and the CCT Review	the Board asks the SSR2 RT to clarify what functionality beyond complaint handling, audits, breach notices, suspensions, and terminations it seeks ICANN Compliance to implement within the scope of the agreements. The Board asks that the SSR2 RT provide greater details on what issues or risks exist from the current operational model, how the SSR2 RT recommendation will address them, and what relevant metrics could be applied to assess implementation. Further, it is unclear what is meant by the terms "performance metrics framework", "guide level of compliance", and "other elements that affect abuse, security, and resilience". The Board suggests that the SSR2 RT provide more detail on the intent of this recommendation to ensure that it is properly considered for implementation. The Board notes that this recommendation may overlap with recommendations from the Initial Report on New gTLD Subsequent Procedures (Section 2.12.3), the Registration Directory Service (RDS)-WHOIS2 Review Final Report and recommendations (4.1, 4.2, and 5.1), and CCT Review Team Final Report recommendations (21). The Board requests clarification on the intent of recommendation 10.1 in light of this potential overlap.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.

Source	SSR2 Section or Rec	Report Section	Comment	Response
RrSG	10.1	Establish a performance metrics framework to guide the level of compliance by Registrars and Registries for WHOIS obligations (including inaccuracy), as well as other elements that affect abuse, security, and resilience, as outlined in the RDS/WHOIS2 Review and the CCT Review.	10.1 - This is already covered by ICANN- Compliance metrics on complaints, Compliance audit, Whois ARS, monitoring by GDD tech team, etc	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
RySG	10.1	Establish a performance metrics framework to guide the level of compliance by Registrars and Registries for WHOIS obligations (including inaccuracy), as well as other elements that affect abuse, security, and resilience, as outlined in the RDS/WHOIS2 Review and the CCT Review.	Compliance-related recommendations must be linked to specific contract terms. “Other elements that affect abuse, security, and resilience” is too vague to be implementable. The RySG believes this is out of scope of SSR2.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
RrSG	10.2	Allocate a specific budget line item for a team of compliance officers tasked with actively undertaking or commissioning the work of performance management tests/assessments of agreed SLA metrics.	10.2 - This is something Compliance already does. A review team, with limited understanding of the operation and structure, should defer to Compliance to determine how it will best allocate resources.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
RySG	10.2	Allocate a specific budget line item for a team of compliance officers tasked with actively undertaking or commissioning the work of performance management tests/assessments of agreed SLA metrics.	The RySG does not see the value in specific compliance officers to handle specific contractual compliance issues. All of Compliance is capable of responding to compliance complaints and ICANN has demonstrated that it’s capable of conducting a full audit of all Ry contracts on a specific issue, like SLAs.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.

Source	SSR2 Section or Rec	Report Section	Comment	Response
SSAC	10.3	Amend the SLA renewal clause from 'automatically renewed' to a cyclical four-year renewal that includes a review clause included (this review period would consider the level of compliance to the performance metrics by the Registrar and Registry and recommend the inclusion of requirements to strengthen the security and resilience where non-compliance was evident).	(3.3.3) Given that the report has noted some challenges relating to enforcement of agreements with contracted parties, it is unclear what the review and the subsequent "recommend the inclusion of requirements" precisely entails. Which party is to perform these reviews? Is it the team envisaged in recommendation 10.2? If not then who would be performing such a review? If so, would these compliance officers possess the skills to be able to, "recommend the inclusion of requirements to strengthen the security and resilience where non-compliance was evident"? Who is to receive the review's recommendations? What criteria would be used by this party to assess these recommendations for additional requirements? If requirements are being proposed, where is the contractual foundation to enforce these requirements? Does recommendation 10.3 implicitly refer to recommendation 15, where changes to the contractual conditions are proposed? Some further clarity on these recommendations would be helpful to understand both the detail of the proposed actions and the overall intent of these recommended measures.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
RrSG	10.3	Amend the SLA renewal clause from 'automatically renewed' to a cyclical four-year renewal that includes a review clause included (this review period would consider the level of compliance to the performance metrics by the Registrar and Registry and recommend the inclusion of requirements to strengthen the security and resilience where non-compliance was evident).	10.3 - It is the position of the RrSG that contract negotiations do not originate from review teams or working groups. That is reserved for ICANN Org, and the RrSG/RySG.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.

Source	SSR2 Section or Rec	Report Section	Comment	Response
RySG	10.3	Amend the SLA renewal clause from 'automatically renewed' to a cyclical four-year renewal that includes a review clause included (this review period would consider the level of compliance to the performance metrics by the Registrar and Registry and recommend the inclusion of requirements to strengthen the security and resilience where non-compliance was evident).	The RySG believes that this is outside the scope of the SSR2's work. The RySG notes that there is an established contract amendment process: consensus policy and negotiations between CPs and ICANN. This recommendation has no basis in policy or fact - it is a conclusory statement that presupposes the question. If the SSR2 has identified problems with performance metrics, then it could recommend that ICANN and the community study them. In this case, the SSR2 is proceeding down the same slippery slope as CCT-RT in recommending solutions without recommending ICANN first engage in exploration and work to determine if a solution is needed.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
RrSG	10.4	Further, the ICANN Board should take responsibility for bringing the EPDP to closure and passing and implementing a WHOIS policy in the year after this report is published.	10.4 - It is not for a review team to determine the pace of the PDPs or IRTs. There can be unexected issues that arise (as during the implementation of EPDP Phase 1), and it is better for ICANN to develop and implement policy properly rather than rushing to meet an artificial deadline.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
RySG	10.4	Further, the ICANN Board should take responsibility for bringing the EPDP to closure and passing and implementing a WHOIS policy in the year after this report is published.	The RySG notes that this recommendation is not made to the appropriate party. A recommendation on a GNSO policy process should be referred to the GNSO Council as the manager of the policy process. Furthermore, it's outside the scope of a review team to recommend that a PDP wrap up (as it undoubtedly will even without the RT's recommendation).	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
GAC	10.4	Further, the ICANN Board should take responsibility for bringing the EPDP to closure and passing and implementing a WHOIS policy in the year after this report is published.	The GAC also agrees with Recommendation 10.4 on implementing the EPDP policy recommendations within 1 year.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
IPC	10.4		While the IPC is supportive of the intent behind recommendation 10.4, it notes that it is not the role of the Board to direct the outcome or timing of a community-led PDP. The RT may wish to revise this language, for example to refer to the Board itself, and via Org, offering all necessary support to achieve the desired outcome	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.

Source	SSR2 Section or Rec	Report Section	Comment	Response
BC	11	Lead Efforts to Evolve Definitions Around Abuse and Enable Reporting Against Those Definitions	The BC concurs with this recommendation and reiterates its previous statements regarding DNS abuse: •...while the BC appreciates the need for actionable definitions of abuse, we are concerned about recent efforts to limit or otherwise over-restrict discussion about the serious issue of domain name system abuse. Such asubject deserves fulsome consideration by the entire community... •ICANN has a responsibility to enforce its contracts in the areas of DNS-related abuse. This community dialogue cannot delay or defer ICANN's commitments or operations related to DNS abuse. •ICANN should clarify the purposes and applications of "abuse" before further work is done to define DNS abuse. •Once those purposes are identified, ICANN should determine whether abuse definitions used by outside sources can serve as references for the ICANN community, or whether a new, outcomes-based nomenclature could be useful (including impersonation, fraud, or other types of abuse) to accurately describe problems being addressed.	Thank you. Please see SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms for revised text for this recommendation.
NCSG	11	Lead Efforts to Evolve Definitions Around Abuse and Enable Reporting Against Those Definitions	#Recommendation 11: As this related to the definition of DNS Abuse, we believe that it is highly important to elaborate more on the methodology and the validation mechanisms.	Thank you. Please see SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms for revised text for this recommendation.
RrSG	11	Lead Efforts to Evolve Definitions Around Abuse and Enable Reporting Against Those Definitions	The RrSG has concerns about this recommendation. The ICANN community is currently engaged in abuse and threat activities, as are the contracted parties. The definition of abuse and threats can be difficult to define broadly, which is perhaps indicitive why there is not a definition that satisfies the review team. It is essential that contracted parties, which have undertanding of implications of these activities, be involved in the process (rather than the ICANN board engaging only security-related community members).	The SSR2 Review Team agrees with this concern. Please see the revised text in Recommendation 10.2. Establish a staff-supported, cross-community working group (CCWG) to establish a process for evolving the definitions of prohibited DNS abuse, at least once every two years, on a predictable schedule (e.g., every other January), that will not take more than 30 business days to complete. This group should involve stakeholders from consumer protection, operational cybersecurity, academic or independent cybersecurity research, law enforcement, and e-commerce.
GAC	11	Lead Efforts to Evolve Definitions Around Abuse and Enable Reporting Against Those Definitions	The GAC welcomes Recommendation 11 on efforts to implement current community vetted definitions of DNS Abuse without delay and the need to ensure that definitions evolve to meet continuing threats, in the context of efforts aimed at finding a more effective approach to address DNS Abuse, including with the GAC's support through its advice, comments, and correspondence. Although the GAC shares the overall goal of achieving clarity and consistency with regard to the definition of DNS Abuse and Security Threats, it is not quite clear how the different processes suggested in Recommendations 11.1, 11.3 and 11.4 should interrelate. The GAC therefore invites the Review Team to consider, in view of existing procedures and rules, how this goal can be best achieved.	The SSR2 Review Team agrees with this assessment. Please see the revised tehxt in SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms.
IPC	11		The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below. As a preliminary matter, the IPC supports SSR2 Recommendation 11: "Lead Efforts to Evolve Definitions Around Abuse and Enable Reporting Against Those Definitions" and any related efforts to define abuse so that reporting and consequences for abuse can flow more efficiently from an agreed-upon definition.	Thank you. Please see SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms for revised text for this recommendation.

Source	SSR2 Section or Rec	Report Section	Comment	Response
SSAC	11		(3.3.1) It is clear that the nature of abuse in the DNS is so pervasive that elimination is not a realistic objective in the foreseeable future. It would be helpful for the report to note the larger picture of abuse and the necessarily scoped range of actions and consequences that lie within ICANN org's area of responsibility so that expectations as to the outcomes of the proposed measures are set to achievable levels.	Thank you. Please see SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms for revised text for this recommendation.
RySG	11.1	ICANN Board should drive efforts that minimize ambiguous language and reach a universally acceptable agreement on abuse, SSR, and security threats in its contracts with contracted parties and implementation plans.	The RySG does not think it is feasible or realistic for there to be "universally acceptable agreement" on definitions for abuse, SSR, and security threats but is willing to continue its extensive ongoing discussions to try to reach such an agreement.	The SSR2 Review Team respectfully disagrees that a universally acceptable agreement on the definitions for abuse, etc, is not feasible. Please see Please see SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms for revised text for this recommendation.
SSAC	11.2	ICANN org and Board should implement the SSR-relevant commitments (along with CCT and RDS/WHOIS2 Review recommendations) based on current, community vetted abuse definitions, without delay	(3.3.4) If the underlying issue is that SSR2 has found evidence that the ICANN Board and ICANN org are not properly processing and acting on the outcomes of other reviews then it should say so explicitly. This recommendation that refers to recommendations from other reviews tends to suggest such a conclusion without actually saying so.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
ICANN Board	11.2	ICANN org and Board should implement the SSR-relevant commitments (along with CCT and RDS/WHOIS2 Review recommendations) based on current, community vetted abuse definitions, without delay	The language of this recommendation presupposes that each of the recommendations are (1) accepted or approved by the ICANN Board; and (2) prioritized by the ICANN community for immediate implementation. The Board notes that it does not believe this to be within scope of the SSR2, and is not aligned with the Bylaws. Additionally, the Board seeks clarification regarding whether this recommendation makes sense in terms of resource deployment in light of the ongoing community discussions regarding the definition of "DNS abuse". The Board also seeks clarification of the information the SSR2 RT has to support its position that the definition of abuse has been vetted through the bottom-up multistakeholder process.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
RySG	11.2	ICANN org and Board should implement the SSR-relevant commitments (along with CCT and RDS/WHOIS2 Review recommendations) based on current, community vetted abuse definitions, without delay	The RySG is unclear about what the SSR2 is asking given Recommendation 1 is to implement the remainder of SSR1 recommendations. We do not support the Board unilaterally adopting the definitions established by either the SSR2, the CCT-RT, or the RDS/WHOIS2 Review without full community adoption.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.

Source	SSR2 Section or Rec	Report Section	Comment	Response
SSAC	11.3	ICANN Board, in parallel, should encourage community attention to evolving the DNS abuse definition (and application), and adopt the additional term and evolving external definition of “security threat”—a term used by the ICANN Domain Abuse Activity Reporting (DAAR) project, and the GAC (in its Beijing Communique and for Specification 11), and addressed in international conventions such as the Convention on Cybercrime and its related “Explanatory Notes” —to use in conjunction with ICANN org’s DNS Abuse definition.	(3.3.5) What specific actions did the SSR2 RT have in mind? It is challenging to understand the intended objectives of this particular recommendation given the imprecision of the term “encourage community attention”.	The SSR2 Review Team has clarified and split this recommendation into two. Please see SSR2 Recommendation 10.1 and 10.2.

Source	SSR2 Section or Rec	Report Section	Comment	Response
ICANN Board	11.3	ICANN Board, in parallel, should encourage community attention to evolving the DNS abuse definition (and application), and adopt the additional term and evolving external definition of “security threat”—a term used by the ICANN Domain Abuse Activity Reporting (DAAR) project, and the GAC (in its Beijing Communique and for Specification 11), and addressed in international conventions such as the Convention on Cybercrime and its related “Explanatory Notes” —to use in conjunction with ICANN org’s DNS Abuse definition.	In reviewing recommendations 11.2 and 11.3 together, the Board requests clarification as to the intent of these recommendations and whether the SSR2 RT believes it prudent to “implement the SSR-relevant commitments (along with CCT and RDS recommendations) based on current, community vetted abuse definitions, without delay”, knowing that the definition may/will evolve. Furthermore, the Board seeks clarification as to how the SSR2 RT would assess effective implementation of this recommendation. It is not clear what the measure of success would be given that the Board cannot mandate the community to reach agreement on the definition of “DNS abuse”. It is also not clear what the SSR2 RT intends for the Board to do in “adopting” a definition. The Board believes that the issue is not about "abuse definition", but about what kind of DNS abuse is within ICANN's remit.	The SSR2 Review Team has revised and clarified this recommendation; please see SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms. Regarding assessing the effective implementation of this recommendation, please note the clarified language of the recommendations themselves and the following summary at the conclusion of the recommendation "This recommendation can be considered effective when ICANN org is able to offer increased transparency and accountability with respect to accepted and community-vetted descriptions and clarity to community discussions and interpretation of policy documents, thus enabling other stakeholders to define codes of conduct around DNS abuse."

Source	SSR2 Section or Rec	Report Section	Comment	Response
RySG	11.3	ICANN Board, in parallel, should encourage community attention to evolving the DNS abuse definition (and application), and adopt the additional term and evolving external definition of “security threat”—a term used by the ICANN Domain Abuse Activity Reporting (DAAR) project, and the GAC (in its Beijing Communique and for Specification 11), and addressed in international conventions such as the Convention on Cybercrime and its related “Explanatory Notes” —to use in conjunction with ICANN org’s DNS Abuse definition.	The RySG believes this work is ongoing but objects to the conclusion of this Recommendation as to which definition the Board should adopt. If 11.3 is to be included as a recommendation, the RySG would only support the text “ICANN Board should encourage community attention to evolving the DNS abuse definition”.	The SSR2 Review Team has clarified and split this recommendation into two. Please see SSR2 Recommendation 10.1 and 10.2, which includes the creation of a cross-community working group to regularly review the definition of abuse.
SSAC	11.4	The ICANN Board should entrust SSAC and PSWG to work with e-crime and abuse experts to evolve the definition of DNS Abuse, taking into account the processes and definitions outlined in the Convention on Cybercrime	(3.3.6) It appears that the part of this recommendation that refers to SSAC actions is already underway with the formation of a DNS Abuse Work Party within SSAC. SSAC would be happy to brief the SSR2 RT on the objectives of this DNS Abuse Work Party. The SSR2 RT should consider whether to retain Recommendation 11.4 or simply note in the report that this activity is underway within SSAC.	The SSR2 Review Team took this comment into consideration and the relevant recommendation has been rewritten. Please see SSR2 Recommendation 10.2.
RySG	11.4	The ICANN Board should entrust SSAC and PSWG to work with e-crime and abuse experts to evolve the definition of DNS Abuse, taking into account the processes and definitions outlined in the Convention on Cybercrime	The RySG believes this is a policy matter and outside the scope of SSR reviews - if the Board would like the community to try to define DNS abuse, then it can instruct the community to do so, but it’s inappropriate to recommend that the definition come solely from two ACs (SSAC and GAC) without input from the rest of the community.	Please see the clarified recommendation in SSR2 Recommendation 10.2 that calls for the creation of a cross-community working group to regularly review the definition of abuse.

Source	SSR2 Section or Rec	Report Section	Comment	Response
BC	12	Create Legal and Appropriate Access Mechanisms to WHOIS Data	The BC concurs with this recommendation but also initially encourages ICANN to begin with proactive review of registrar compliance with the Temp Spec. The Compliance team could start with review of redaction of data, easy-to-find reveal request policies on registrar websites and average response time to requests for registrant data.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
NCSG	12	Create Legal and Appropriate Access Mechanisms to WHOIS Data	#Recommandation 12: This recommendation is outside of the review team remit and is already addressed by current ICANN Policymaking in the GNSO and thus should be removed.	The review team believes that WHOIS is extremely relevant to security, stability, and resiliency and is therefore within the remit of the SSR2 review. Please see SSR2 Recommendation 16.2 for revised text.
WIPO	12	Create Legal and Appropriate Access Mechanisms to WHOIS Data	ICANN's continued delay in facilitating a centrally-coordinated mechanism for standardized access to non-public registrant data is harming a range of legitimate causes, including law enforcement, security researchers, and intellectual property owners and consumers.1 Beyond fostering scalability and predictability in all stakeholders' interests, developing such an access model would remove a current risk faced by Contracted Parties in assessing WHOIS disclosure requests.2	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
RySG	12	Create Legal and Appropriate Access Mechanisms to WHOIS Data	The RySG does not support SSR2 making this recommendation given the ongoing EPDP Phase 2 work and questions how this falls within the scope of this review.	The review team believes that WHOIS is extremely relevant to security, stability, and resiliency and is therefore within the remit of the SSR2 review. Please see SSR2 Recommendation 16.2 for revised text.
IPC	12		The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below. The IPC strongly supports the RT's recommendations that address investigating and responding to DNS abuse, including Recommendation 12: "Create Legal and Appropriate Access Mechanisms to WHOIS Data," SSR2 Recommendation 13: "Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program (DAAR)," SSR2 Recommendation 17: "Establish a Central Abuse Report Portal," and SSR2 Recommendation 19: "Update Handling of Abusive Naming." Recommendation 12 addressing WHOIS data addresses issues raised by many in the community including the Security and Stability Advisory Committee (SSAC), Governmental Advisory Committee (GAC), BC, and IPC. It is important to the issue of addressing abuse that registrant data is correct, and available through the proper channels or to the proper authorities.	The SSR2 Review Team's recommendations regarding compliance and abuse have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
SSAC	12.1	The ICANN Board should create a legal and appropriate access mechanisms to WHOIS data by vetted parties such as law enforcement.	(3.3.7) The SSAC largely agrees with the intent of this recommendation, while noting that this measure admits the risk of unintended consequences when considering the generality of the Internet and the diversity of bodies that enforce national regulations. How could ICANN minimize such risks in the context of the implementation of this recommendation?... This general recommendation appears not to take into account the existing activities in this area.	Thank you. Please see the revised recommendation in SSR2 Recommendation 16.2.
RrSG	12.1	The ICANN Board should create a legal and appropriate access mechanisms to WHOIS data by vetted parties such as law enforcement.	Regarding recommendation 12.1, this is currently being addressed by EPDP Phase 2, and should not be subject to another PDP.	This feedback has been taken into account in the revised recommendation. Please see the revised recommendation in SSR2 Recommendation 16.2.

Source	SSR2 Section or Rec	Report Section	Comment	Response
RrSG	12.2	The ICANN Board should take responsibility for, and ensure ICANN org comes to immediate closure on, implementation of the Temporary Specification for gTLD Registration Data.	For recommendation 12.2, as indicated previously, there is a pending IRT that is dealing with complex issues. The IRT should be allowed to proceed at its current pace to ensure quality outcome (rather than rushing to meet an artificial deadline).	This feedback has been taken into account in the revised recommendation. Please see the revised recommendation in SSR2 Recommendation 16.2.
BC	13	Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program	The BC concurs with this recommendation. The DAAR program is one of unrealized potential. Executed well, DAAR would have the capability of informing ICANN (and the community) with precision regarding the source (s) of abusive behavior, making it easier to enlist the cooperation of contracted parties in mitigation efforts. The BC encourages ICANN Org to invest further in an improved and robust DAAR program, and encourages the ICANN Board to lend its support and oversight to the effort.	Thank you. Please see the revised text in SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review.
M3AAWG	13	Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program	(5) We recommend that the SSR2 make clear that rate limiting is an impediment to the DAAR system's ability to accurately report registrar statistics.	This portion of the report has been significantly rewritten, and this specific point was too low-level for inclusion in the revised text. Please see the revised text in SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review.
SSAC	13	Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program	(3.3.8) It is unclear if "completeness" here refers to the limited realm of second level domain names in gTLDs. If the intent is a far broader scope of "completeness" including all top-level domains (TLDs) and all labels to an arbitrary depth of delegation, then it would be helpful if the report indicated how such an extension of this activity could take place. Also, the draft report should clearly indicate what is actionable with the specific recommendations, and more precisely, how effectiveness can be measured. Who should get the Domain Abuse Activity Reporting (DAAR) reports, and what should be made public, needs further attention in this recommendation. The SSAC suggests that further consultation within the ICANN community on DAAR methodologies would be helpful.	Thank you. Please see the revised text in SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review.
WIPO	13	Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program	To the extent ICANN would consider UDRP cases as part of any DAAR or Domain Name Marketplace Indicators, it should be noted that while the UDRP supports consumer trust, this is trust earned only after significant time and expense is invested by brand owners (and in some cases only after a fraud has been perpetrated on end users). The continued availability of the UDRP, as operated by WIPO on a not-for-profit basis, moreover benefits Contracted Parties and ICANN by keeping them out of disputes. The fact that WIPO has seen record-breaking numbers of UDRP cases over the years illustrates that the root issue of cybersquatting is not itself being addressed. To this end ICANN may wish to look at programs instituted in the .EU and .DK domain spaces.	This portion of the report has been significantly rewritten, and cybersquatting as a specific point was too low-level for inclusion in the revised text. Please see the revised text in SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review.
ICANN Org	13	Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program	Work is already underway by ICANN org towards implementation of this recommendation. If the SSR2 RT's intent is to recommend implementation of something beyond what is in progress with ongoing work, ICANN org encourages the SSR2 RT to provide specific details.	Thank you. Please see the revised text in SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review.

Source	SSR2 Section or Rec	Report Section	Comment	Response
IPC	13		The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below. The IPC strongly supports the RT's recommendations that address investigating and responding to DNS abuse, including Recommendation 12: "Create Legal and Appropriate Access Mechanisms to WHOIS Data," SSR2 Recommendation 13: "Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program (DAAR)," SSR2 Recommendation 17: "Establish a Central Abuse Report Portal," and SSR2 Recommendation 19: "Update Handling of Abusive Naming." ... As for the DAAR, the IPC commends ICANN's intended goal of "develop [ing] a robust, reliable, reproducible, and replicable methodology for analyzing security threat activity that can then be later used by the ICANN community to facilitate informed policy decisions." However, the RT's assessment finds that the DAAR falls far short of this goal in practice because it lacks sufficient information to be able to tell which registrars or registries are harboring significant abuse. The IPC supports the RT's recommendation to include this critical data and turn the DAAR into a powerful tool for accountability and transparency in the domain name registration system. ... The IPC does however note that a number of brand owners now operate Brand TLDs under Specification 13, in which, due to the nature of these TLDs, the risk of DNS abuse is low. In making recommendations that seek to impose additional obligations for monitoring and reporting, the IPC would urge the RT to acknowledge differing risk profiles and avoid imposing unnecessary and costly burdens on Brand TLDs. In particular, this might include different requirements for access to Brand TLD zone files through the CZDS, different security threat monitoring and reporting requirements, and different audit approaches with respect to maintaining the security of a Brand TLD.	Thank you. Please see the revised recommendations in Section E. Contracts, Compliance, and Transparency around DNS Abuse, in particular SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review, SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting, and SSR2 Recommendation 16: Privacy Requirements and RDS.
RrSG	13.1	The ICANN Board and ICANN org should work with the entities inside and outside the ICANN community that are mitigating abuse to improve the completeness and utility of DAAR, in order to improve both measurement and reporting of domain abuse.	Regarding recommendation 13.1, this data is already being published elsewhere. It is outside of ICANN's scope to aggregate and republish this data. It is also not clear that DAAR is incomplete or ineffective, so additional information is needed to know how the cost for these additional resources outweighs any benefit.	The SSR2 Review Team respectfully disagrees that aggregating and republishing data is outside ICANN's scope. Please see E.2.a.iii. DNS Abuse Activity Reporting for updated text on this matter.

Source	SSR2 Section or Rec	Report Section	Comment	Response
ICANN Org	13.1	The ICANN Board and ICANN org should work with the entities inside and outside the ICANN community that are mitigating abuse to improve the completeness and utility of DAAR, in order to improve both measurement and reporting of domain abuse.	ICANN org solicits input from all stakeholders on how to improve DAAR on a regular basis, including via daar@icann.org and the “DNS abuse measurements” mailing list	The SSR2 Review Team respectfully disagrees with this feedback. Available information indicates a lack of outreach outside the ICANN community, and a lack of follow-through on input from non-contracted parties who want to improve both measurement and reporting of domain abuse. Please see E.2.a.iii. DNS Abuse Activity Reporting for updated text on this matter.
RySG	13.1		The RySG notes that the ONLY entities that can take down domain name abuse are: registries, registrars, hosts, and registrants. There are no third parties that mitigate abuse: only third party tools that analyze data and report on that data.	The SSR2 Review Team notes that abuse take downs are a seperate issue from measurement and reporting of abuse. Please see the clarified text in SSR2 Recommendation 12.1
ICANN Org	13.2	ICANN Board should annually solicit and publish feedback from entities inside and outside the ICANN community that are mitigating abuse in order to help enhance ICANN org’s data on domain abuse activity.	This appears to be duplicative of 13.1. ICANN org encourages the SSR2 RT to clarify the differences in these two recommendations.	Thank you. Please see the revised text in SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review.
BC	14	Enable Rigorous Quantitative Analysis of the Relationship Between Payments for Domain Registrations and Evidence of Security Threats and Abuse	While the BC historically has discouraged ICANN Org from engaging on matters of pricing, thisdata could be informative and helpful in identifying and targeting sources of DNS abuse. The BC supports.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
SSAC	14	Enable Rigorous Quantitative Analysis of the Relationship Between Payments for Domain Registrations and Evidence of Security Threats and Abuse	(3.3.9) Given that ICANN has deliberately distanced itself from any role as a regulator of pricing in this space and holds a position where market forces determine pricing, then what is the context of this analysis and how could such a rigorous quantitative analysis inform the mechanisms of market-based pricing? Further elaboration of the envisaged use of such an analysis would be useful to understand the intended effect of this recommendation. If this recommendation is an oblique reference to heavily discounted prices being applied to bulk name registration practices, then is the underlying abuse issue pricing or bulk registration?	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.

Source	SSR2 Section or Rec	Report Section	Comment	Response
RrSG	14	Enable Rigorous Quantitative Analysis of the Relationship Between Payments for Domain Registrations and Evidence of Security Threats and Abuse	The RrSG notes that this was already recommended by CCT. The ICANN board deferred implementing and stated "questions raised regarding the value of the data" (see https://www.icann.org/en/system/files/files/resolutions-final-cct-recs-scorecard-01mar19-en.pdf). It is not clear what will be accomplished by collecting this information. There are extensive reports already that tie low cost, or free registrations to abuse activity (which are havens for abusive domains, along with low cost hosting). Additionally, ICANN is likely not in a position to determine a full picture due to the large and varying promotional pricing, or prices set by resellers of registrars, or for registrars that do not provide this information publicly. This could be a massive undertaking which might not produce useful information.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
WIPO	14	Enable Rigorous Quantitative Analysis of the Relationship Between Payments for Domain Registrations and Evidence of Security Threats and Abuse	Part of any meaningful look at payments for domains used to perpetuate abuse would also look at data accuracy under the umbrella of anti-fraud know-your-customer norms (which would in turn call for a timely resolution of PPSAI independent of EPDP work).	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
RySG	14	Enable Rigorous Quantitative Analysis of the Relationship Between Payments for Domain Registrations and Evidence of Security Threats and Abuse	The RySG does not support this recommendation as it is out of SSR2's remit. The RySG notes that ICANN is not a price regulator and is unclear what benefit would come from this research. Further, the RySG is concerned that this recommendation presupposes a relationship between the price of domain names and evidence of "security threats and abuse". The RySG refers to its previous comments on collecting pricing data made in response to the CCT-RT Final Report, particularly recommendations 2, 3, and 4.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
IPC	14		The IPC is supportive of this recommendation.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
ICANN Board	14.1	ICANN org should collect, analyze, and publish pricing data to enable further independent studies and tracking of the relationship between pricing and abuse	The Board notes that this recommendation seems to raise similar questions the Board noted when considering recommendations from the CCT Review Team about collecting pricing data (see page 4 of the scorecard with regard to CCT recommendations 3 and 4). With regard to the relevant CCT Review Team recommendations, the Board placed them in "Pending" status, and directed ICANN org, through engagement of a third party, to conduct an analysis to identify what types of data would be relevant in examining the potential impacts on competition and, whether that data is available, and how it could be collected in order to benefit the work of future CCT Review Teams. The Board stated that this analysis would inform the Board's decision on next steps and whether the recommendations could be adopted. Given this background, the Board would like to understand whether the SSR2 RT has considered the Board's previous concerns and how that has been factored into its deliberations.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.

Source	SSR2 Section or Rec	Report Section	Comment	Response
IPC	14.1		While the IPC is strongly supportive of the intent behind recommendation 14.1, it notes that new gTLD registries are not under a contractual obligation to disclose their wholesale pricing and that efforts to gather this information from registries voluntarily during previous reviews (such as CCT) and PDPs (such as RPMs) have been unsuccessful. The RT is encouraged to revisit and refine this recommendation, for example to encourage Org to seek to include obligations during contract renewal/contract negotiations to disclose pricing information on a confidential basis for the use by RTs and PDPs and/or for Org to consider whether registrar retail pricing can meaningfully inform this issue.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
BC	15	Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse	The BC concurs with this recommendation. The BC underlines its previous comments(dating back to input on the CCT review team's findings in late 2018) regarding the establishment of thresholds of abuse harboring and a corresponding instigation of compliance inquiries. The BC believes the problem of abuse is acute enough, and growing fast enough, to warrant such a system, and encourages the contractual changes. For the same reason, the BC agrees with recommendation 15.2 regarding contract termination. With regard to the suite of recommendations under 15.3, the BC concurs here as well --particularly 15.3.1.The European Union's (EU) General Data Protection Regulation (GDPR) has decimated the investigatory value of the Whois database.The BC reiterates its many inputs calling for sensible access to non-public Whois data, with vigorous enforcement of that access right given to ICANN as a compliance matter 15.4 also is a particularly useful recommendation in that it seeks to codify in contracts the necessity of addressing DNS abuse as the serious matter that it is. While the BC has applauded the several contracted parties who voluntarily have adopted a framework for addressing abuse, the situation unfortunately requires assertive mandates as a way of truly rooting out abuse.	Thank you. Please see the revised recommendations in Section E. Contracts, Compliance, and Transparency around DNS Abuse, in particular SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review, SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting, and SSR2 Recommendation 16: Privacy Requirements and RDS.
M3AAWG	15	In its review of ICANN org's activities, the SSR2 RT found that the publications, statements, and related actions by ICANN org have consistently understated or omitted the impact of systemic abuse of the DNS and its use as a platform for launching systematic attacks on individual and organizational systems worldwide.	(intro) We concur with the SSR2 RT assertion that "the publications, statements, and related actions by the ICANN organization have consistently understated or omitted the impact of systemic abuse of the DNS and its use as a platform for launching systematic attacks on individual and organizational systems worldwide". The report should further urge the ICANN organization to be transparent and to exercise its ability "to negotiate, enter into and enforce agreements, including public interest commitments, with any party in service of its Mission" (See ICANN Bylaws, Article 1, Mission at https://www.icann.org/resources/pages/governance/bylaws-en/#article1).	Thank you. Please see the revised recommendations in Section E. Contracts, Compliance, and Transparency around DNS Abuse, in particular SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review, SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting, and SSR2 Recommendation 16: Privacy Requirements and RDS.
M3AAWG	15		(3) We recommend that the SSR2 RT urge ICANN to adopt a contract negotiation process in which the influence of contracted parties who pay fees to ICANN cannot be held in question.	Thank you, this has been incorporated. Please see SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties.

Source	SSR2 Section or Rec	Report Section	Comment	Response
M3AAWG	15		(4) We urge the SSR2 RT to recommend that contracted parties be obligated by contract to accommodate the high-volume needs of operational security users. Mechanisms such as whitelisting, vetting or pre-authorization which unfairly encumber academics, individuals who responsibly investigate abuse, and generally any party who has legitimate purposes to collect registration data, should not be used.	Thank you. This section of the report has seen significant reorganization. The report call for the "validation, transparency, and independent reproducibility of analyses"; however, it does not insist on high-volume access for any particular set of users. Please see the revised recommendations in Section E. Contracts, Compliance, and Transparency around DNS Abuse, in particular SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements.
SSAC	15	Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse	(3.3.10) This appears to be a more detailed and clearer restatement of Recommendation 10.3, and in this light Recommendation 10.3 appears to be somewhat unnecessary.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and in particular SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review, SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting, and SSR2 Recommendation 16: Privacy Requirements and RDS.
RrSG	15	Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse	It is the position of the RrSG that contract negotiations should originate through ICANN, the RrSG, and the RySG, rather than a review team. Any recommendations for changes to the RAA or RA are out of scope.	The review team has recommended actions that we believe are within our Bylaws-mandate and scope to improve SSR and serve the public interest. Please see our mapping of recommendations back to ICANN's Bylaws and Strategic Plan: Appendix G: Mapping of SSR2 Recommendations to the ICANN 2021-2025 Strategic Plan and the ICANN Bylaws.
WIPO	15	Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse	ICANN could consider incentives such as “audit credits” to incentivize adoption of best practices.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
RySG	15	Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse	The SSR RT has no authority to make recommendations to enhance or make changes to the Registry or the Registrar Accreditation Agreements and strongly objects to this set of recommendations. Similarly, the ICANN Board has no authority to implement the recommendation/s. The RySG opposes this recommendation because it presupposes the outcome of work that should be done by the community and, in several places, seems to try to preempt (and end-run around) work being done in the community and by other PDPs, such as the EPDP. Furthermore this recommendation is wholly outside the scope of the SSR2’s remit (e.g. setting threshold to trigger “automatic” contract defaults). Perhaps the scope of SSR3 will be to review the outcome of the various work in progress today, but this RT is not tasked with using the Recommendations of the RT to hammer home viewpoints on how the Board and the community should presume to resolve ongoing work.	The review team has recommended actions that we believe are within our Bylaws-mandate and scope to improve SSR and serve the public interest. Please see our mapping of recommendations back to ICANN's Bylaws and Strategic Plan: Appendix G: Mapping of SSR2 Recommendations to the ICANN 2021-2025 Strategic Plan and the ICANN Bylaws.

Source	SSR2 Section or Rec	Report Section	Comment	Response
IPC	15		The IPC is generally supportive of this recommendation, and discusses its support for this recommendation in greater detail below. The RT recommends, and the IPC supports, several methods for ICANN to better utilize its relationships with the Registrars and Registries to combat DNS abuse, including SSR2 Recommendation 10: “Improve the Framework to Define and Measure Registrar & Registry Compliance,” SSR2 Recommendation 15: “Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse,” and SSR2 Recommendation 16: “Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats.” The IPC supports these recommendations and any steps to more effectively combat DNS abuse relating to the Registry Agreement (RA) and Registrar Accreditation Agreement (RAA) contracts. ... Accordingly, the IPC supports these SSR2 recommendations that would require meaningful enforcement of existing obligations of registries and registrars to prohibit certain security threats and abusive activities, enhance such requirements to further mitigate such activities, include real consequences for registrants who engage in prohibited abusive behavior, and motivate active and consistent investigation and response to reports of abuse by registrars.	Thank you. Please see the revised recommendations in Section E. Contracts, Compliance, and Transparency around DNS Abuse, in particular SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties, SSR2 Recommendation 9: Monitor and Enforce Compliance, SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms, and SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting.
ICANN Board	15.1	ICANN org should, make SSR requirements mandatory on contract or baseline agreement renewal in agreements with contracted parties, including Registry Agreements (base and individual) and the RAA, These contract requirements should include provisions that establish thresholds of abuse (e.g., 3% of all registrations) that would automatically trigger compliance inquiries, with a higher threshold (e.g., 10% of all registrations) at which ICANN org considers registrars and registries to be in default of their agreements. The CCT Review also recommended this approach	As noted with regard to SSR2 recommendation 11.2, the Board seeks clarification regarding whether this recommendation would be reasonable in terms of resource deployment in light of the ongoing community discussions regarding the definition of "DNS abuse". Further, as noted above, the Board cannot unilaterally impose new obligations on contracted parties through acceptance of a recommendation from the SSR2 RT. The Registry Agreement and Registrar Accreditation Agreement (RAA) can be modified either via a consensus policy development process or as a result of voluntary contract negotiations. In either case, the Board does not have the ability to ensure a particular outcome.	The SSR2 Review Team has revised this recommendation. Please see SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements.

Source	SSR2 Section or Rec	Report Section	Comment	Response
ICANN Org	15.1	ICANN org should, make SSR requirements mandatory on contract or baseline agreement renewal in agreements with contracted parties, including Registry Agreements (base and individual) and the RAA, These contract requirements should include provisions that establish thresholds of abuse (e.g., 3% of all registrations) that would automatically trigger compliance inquiries, with a higher threshold (e.g., 10% of all registrations) at which ICANN org considers registrars and registries to be in default of their agreements. The CCT Review also recommended this approach.	ICANN org notes it is unable to unilaterally “make SSR requirements mandatory...”. Neither ICANN org nor the Board can unilaterally impose new obligations on contracted parties. The Registry Agreement (RA) and Registrar Accreditation Agreement (RAA) can only be modified either via a consensus policy development process or as a result of voluntary contract negotiations (as noted by the Board). ... ICANN org therefore encourages the SSR2 RT to consider the ongoing community discussions regarding the definition of "DNS abuse" and how to measure “DNS abuse” through metrics and reporting in finalizing this recommendation, as noted by the Board.	The SSR2 Review Team has revised this recommendation. Please see SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements.
RrSG	15.4	In the longer term, ICANN Board should request that the GNSO initiate the process to adopt new policies and agreements with Contracted Parties that measurably improve mitigation of DNS abuse and security threats, including changes to RDAP and registrant information, incentives for contracted parties for abuse/security threat mitigation, establishment of a performance metrics framework, and institutionalize training and certifications for contracted parties and key stakeholders	For recommendation 15.4, the RrSG supports the use of the GNSO to develop ICANN policy.	The SSR2 Review Team agrees with this comment, and has recommended a more balanced GNSO and PDP process is needed. Please see SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements.

Source	SSR2 Section or Rec	Report Section	Comment	Response
BC	16	Create Pricing Incentive	The BC applauds this common sense recommendation and encourages ICANN Org and the Board to institute incentive policies as a matter of priority.	Thank you. Please see SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements for revised text.
M3AAWG	16	Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats	(7) Make all forms of pricing, including promotional pricing and bulk registration pricing, a matter of public record and “open data”. We concur with the SSR2 RT recommendation that ICANN should study pricing, yet urge the review team to further ask that registries and registrars share pricing with ICANN as a matter of contract, and that ICANN publish pricing at its web site, in machine usable formats.	Thank you. Please see SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements for revised text.
M3AAWG	16	Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats	(8) We urge the SSR2 team to call for further economic modeling and study of the DNS economy by qualified professionals instead of explicit pricing recommendations.	Thank you. Please see SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements for revised text.
SSAC	16	Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats	(3.3.11) The SSAC notes that this recommendation may be premature, as it presupposes the results from the activity proposed in Recommendation 14. The SSAC has some concerns regarding the propriety and practicality of this recommendation. This proposal may transfer abuse behaviour into those parts of the domain name space that are not directly subject to the same incentives and constraints. Such a program may be extremely difficult to manage and its effectiveness difficult to measure. This recommendation also proposes a shift of ICANN’s role, as ICANN has moved away from a price regulatory role and towards an environment where pricing is a function of market dynamics. ...	Thank you. Please see SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements for revised text.
RrSG	16	Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats	While this recommendation appears to be a good start, it must be subject to a PDP to determine if incentives are a good mechanism to address security threats. As for incentives, they are usually subject to abuse itself and or gaming (and bad actors will figure out a way around it).	Thank you. Please see SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements for revised text.
ICANN Org	16	Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats	ICANN org notes that neither it nor the Board can unilaterally impose new obligations on contracted parties. The RA and RAA can only be modified either via a consensus policy development process or as a result of voluntary contract negotiations (as noted by the Board). Further, ICANN org encourages the SSR2 RT to consider and describe what the likely externalities of incentivizing certain behavior might be so that the ICANN org and Board may comprehensively assess the impacts of the implementation of this recommendation.	The Board has several options available to it as described in the revised recommendations SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements.
RySG	16	Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats	Again, the RySG opposes this recommendation because it’s outside the scope of the RT’s role.	The review team has recommended actions that we believe are within our Bylaws-mandate and scope to improve SSR and serve the public interest. Please see our mapping of recommendations back to ICANN's Bylaws and Strategic Plan: Appendix G: Mapping of SSR2 Recommendations to the ICANN 2021-2025 Strategic Plan and the ICANN Bylaws.

Source	SSR2 Section or Rec	Report Section	Comment	Response
IPC	16		The IPC is generally supportive of this recommendation, and discusses its support for this recommendation in greater detail below. The RT recommends, and the IPC supports, several methods for ICANN to better utilize its relationships with the Registrars and Registries to combat DNS abuse, including SSR2 Recommendation 10: "Improve the Framework to Define and Measure Registrar & Registry Compliance," SSR2 Recommendation 15: "Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse," and SSR2 Recommendation 16: "Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats." The IPC supports these recommendations and any steps to more effectively combat DNS abuse relating to the Registry Agreement (RA) and Registrar Accreditation Agreement (RAA) contracts. ... Accordingly, the IPC supports these SSR2 recommendations that would require meaningful enforcement of existing obligations of registries and registrars to prohibit certain security threats and abusive activities, enhance such requirements to further mitigate such activities, include real consequences for registrants who engage in prohibited abusive behavior, and motivate active and consistent investigation and response to reports of abuse by registrars.	Thank you. Please see the revised recommendations in Section E. Contracts, Compliance, and Transparency around DNS Abuse, in particular SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties, SSR2 Recommendation 9: Monitor and Enforce Compliance, SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms, SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting, SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements, and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements.
ICANN Org	16.1	SSR2 Recommendation 16.1: "commercial providers"	Requests for clarification of terms	This term is no longer used in the report.
ICANN Org	16.1	Contracted parties with portfolios with less than a specific percentage (e.g., 1%) of abusive domain names (as identified by commercial providers or DAAR) should receive a fee reduction (e.g., a reduction from current fees, or an increase of the current per domain name transaction fee and provide a Registrar with a discount).	As noted in the section "Requests for Clarification of Terms," ICANN seeks clarification regarding the term "commercial providers". ICANN org also notes that this recommendation may overlap with ongoing work related to the Competition, Consumer Trust, and Consumer Choice Review Team (CCT RT) recommendations. The Board passed through CCT recommendation 12 regarding incentives to the New gTLD Subsequent Procedures PDP Working Group (see page 2 of the scorecard). ICANN org encourages the SSR2 RT to consider the ongoing work of the New gTLD Subsequent Procedures PDP Working Group with regard to applicant fees and whether this recommendation may overlap with that work.	The SSR2 RT considered ongoing work up to January 2020. In order to finish the report, the RT needed to stop tracking and considering additional information about ongoing activities.

Source	SSR2 Section or Rec	Report Section	Comment	Response
RrSG	16.2	Given all parties (ICANN org, contracted parties, and other critical stakeholders such as Registries, Registrars, Privacy/Proxy Service Providers, Internet Service Providers, and the contracted parties) must understand how to accurately measure, track, detect, and identify DNS abuse, ICANN org should institutionalize training and certifications all parties in areas identified by DAAR and other sources on the common methods of abuse [citation to be added] and how to establish appropriate mitigation efforts. Training should include as a starting point: Automatic tracking of complaint numbers and treatment of complaints; Quarterly/Yearly public reports on complaints and actions; and analysis.	Recommendation 16.2 is outside of ICANN's remit, and the source of funding for this is not clear (e.g. what would ICANN cancel to pay for this).	The SSR2 Review Team disagrees that recommendations regarding contracted parties and other stakeholders are outside of the team's remit. Clarifications have been added, however. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.

Source	SSR2 Section or Rec	Report Section	Comment	Response
ICANN Org	16.2	Given all parties (ICANN org, contracted parties, and other critical stakeholders such as Registries, Registrars, Privacy/Proxy Service Providers, Internet Service Providers, and the contracted parties) must understand how to accurately measure, track, detect, and identify DNS abuse, ICANN org should institutionalize training and certifications all parties in areas identified by DAAR and other sources on the common methods of abuse [citation to be added] and how to establish appropriate mitigation efforts. Training should include as a starting point: Automatic tracking of complaint numbers and treatment of complaints; Quarterly/Yearly public reports on complaints and actions; and analysis.	ICANN notes that both in Recommendation 15.4 and 16.2, the SSR2 RT recommends that ICANN org "institutionalize training and certifications." ICANN org requests clarification regarding the SSR2 RT's expectations for training and certifications (i.e., types, methods) as well as the intended meaning of "institutionalize." Is the SSR2 RT requesting that general training courses be offered, for example through ICANN Learn, regarding SSR-related topics such as abuse? ... Is the intent of the SSR2 RT's recommendation to go beyond such activities? Is the SSR2 RT recommending that a more formal certification program be created, where, upon completion, parties are "ICANN-certified" in SSR-related issue mitigation? It is not clear who the intended audience of the training and certification is as the SSR2 RT mentions several parties. Would training and certification be offered to any interested party? Depending on the SSR2 RT's expectations, ICANN org has concerns with the feasibility of implementing such global certification programs. Finally, if the SSR2 RT is referring to more stringent requirements to complete training or certification, such as potential obligations in contracts, this is not within ICANN org's remit to unilaterally impose, as such changes could only come about via consensus policy development or voluntary contract negotiations (as noted by the Board).	To implement industry security standards (ITIL, ISO 27000 family, SSAE-18), ICANN org will identify the training and certifications that are needed. The recommendation expects this information to be available to the community. Please see the revised text in Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
BC	17	Establish a Central Abuse Report Portal	The BC concurs with this recommendation.	Thank you. Please see updated text in SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting.
RrSG	17	Establish a Central Abuse Report Portal	It is not clear what are the "relevant parties" in this recommendation. If only registrars and registries, then such a system will likely cost more than any perceived benefit. If it is intended that it would be all inclusive (e.g. P/P providers, hosting providers, etc), it would be outside of ICANN's scope.	This text has been clarified. Please see updated text in SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting.
WIPO	17	Establish a Central Abuse Report Portal	In addition to a Central Abuse Report Portal, any measures that ICANN or a Contracted Party implements to address a reported abuse should be published along with the responses.	This text has been clarified. Please see updated text in SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting.
RySG	17	Establish a Central Abuse Report Portal	The Registry Agreement requires an email abuse point of contact (POC) on a per-registry basis. Any change to this requirement needs to be the result of a PDP or contract amendment. The RySG further reiterates its concern with the use of the "abuse" terminology in this recommendation. The RySG is also unsure why the responses must be publicly searchable, especially considering that they may contain confidential, sensitive or personal information, and that the disclosure of such information could disrupt in-process law enforcement investigations or violate the privacy rights of data subjects.	This text has been clarified. Please see updated text in SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting.

Source	SSR2 Section or Rec	Report Section	Comment	Response
IPC	17		The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below. The IPC strongly supports the RT's recommendations that address investigating and responding to DNS abuse, including Recommendation 12: "Create Legal and Appropriate Access Mechanisms to WHOIS Data," SSR2 Recommendation 13: "Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program (DAAR)," SSR2 Recommendation 17: "Establish a Central Abuse Report Portal," and SSR2 Recommendation 19: "Update Handling of Abusive Naming." Recommendation 12 addressing WHOIS data addresses issues raised by many in the community including the Security and Stability Advisory Committee (SSAC), Governmental Advisory Committee (GAC), BC, and IPC. It is important to the issue of addressing abuse that registrant data is correct, and available through the proper channels or to the proper authorities.	Thank you. Please see the revised recommendations in Section E. Contracts, Compliance, and Transparency around DNS Abuse, in particular SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties, SSR2 Recommendation 9: Monitor and Enforce Compliance, SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms, SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting, SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements, and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements.
SSAC	17.1	ICANN org should establish and maintain a central DNS abuse complaint portal that automatically directs all abuse reports to relevant parties. The system would purely act as inflow, with only summary and metadata flowing upstream. Use of the system should be mandatory for all gTLDs; ccTLDs should be invited to join. Responses must be publicly searchable and included in yearly reports (in complete form, or by reference). In addition, reports should be made available (e.g., via email) to non-participating ccTLDs.	(3.3.12) The SSAC suggests that this recommendation be given a clearer rationale and also should note that any implementation of such a measure should carefully mitigate the inherent risks of undertaking this role of intermediary in abuse reporting.	Please see the revised rationale in Section E.1.a.iv. Complaints and the revised recommendation in SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting .
ICANN Org	17.1	SSR2 Recommendation 17.1: "abuse report"	Requests for clarification of terms	This text has been clarified. The review team believes that the total answer for the definition is in the mind of the person submitting the complaint; they would not be submitting a report if they did not think it was a situation of abuse. Please see updated text in SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting.

Source	SSR2 Section or Rec	Report Section	Comment	Response
ICANN Org	17.1	ICANN org should establish and maintain a central DNS abuse complaint portal that automatically directs all abuse reports to relevant parties. The system would purely act as inflow, with only summary and metadata flowing upstream. Use of the system should be mandatory for all gTLDs; ccTLDs should be invited to join. Responses must be publicly searchable and included in yearly reports (in complete form, or by reference). In addition, reports should be made available (e.g., via email) to non-participating ccTLDs.	ICANN org notes that there are no details or rationale for this recommendation in the “ICANN Compliance” section of the SSR2 draft report. It is difficult for ICANN org to determine how the review team envisions the operational details and measures of success for this recommendation. For this reason, ICANN org encourages the SSR2 RT to clarify the identified issues or risks that led to this draft recommendation, how the recommended solution will address these issues or risks, the expected impact of implementation, or what relevant metrics could be applied to assess implementation.	Please see the revised rationale in Section E.1.a.iv. Complaints and the revised recommendation in SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting .
BC	18	Ensure that the ICANN Compliance Activities are Neutral and Effective	The BC concurs with this recommendation. For too long, ICANN’s compliance function has been notoriously weak.The BC supports the Board’s investiture of additional power into Compliance, and further supports greater accountability by Compliance through the adherence to SLAs. If ICANN is to do its part in mitigating DNS abuse, it musthave an effective, accountable compliance function; further, to ensure activities are effective, ICANN’s contracts with registries and registrars must be in order and enforceableby compliance	Thank you. Please see the revised recommendations in SSR2 Recommendation 9: Monitor and Enforce Compliance.
SSAC	18	Ensure that the ICANN Compliance Activities are Neutral and Effective	(3.3.13) The SSAC is unsure of how this recommendation materially differs from Recommendations 10 and 15.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
WIPO	18	Ensure that the ICANN Compliance Activities are Neutral and Effective	To support the recommendation of ICANN increasing its Compliance efforts, serious considerationshould be given to addressing – to use ICANN’s word – the “discrepancy” identified in ICANN’s letter of February 12, 2020 to the Business Constituency that ICANN’s compliance obligations are limited to ensuring that a registrar includes an abuse policy clause in its registration agreement. Such self-imposed limitation can hardly be said to underpin a compliance program that is stated to support the security and stability of the global Internet, upon which business and consumers rely.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.

Source	SSR2 Section or Rec	Report Section	Comment	Response
RySG	18	Ensure that the ICANN Compliance Activities are Neutral and Effective	The RySG is unclear why this recommendation is being made. Although SSR2 flags that the contractual obligations are implemented differently by each contracted party, the RySG notes that the contracts do not prescribe uniform or required mechanisms for contracted parties to meet their obligations. There is presently no SLA that can be pointed to in order to determine, unequivocally, that a contracted party is “aiding and abetting systemic abuse,” nor does it make sense to try to measure contracted party behavior in this way. This recommendation should be reconsidered.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
IPC	18		The IPC is supportive of this recommendation.	Thank you. Please see the revised recommendations in SSR2 Recommendation 9: Monitor and Enforce Compliance.
RrSG	18.1	ICANN org should have compliance activities audited externally and hold them to a high standard.	Regarding recommendation 18.1, the RrSG supports that ICANN Compliance should be subject to outside audit.	Thank you. Please see the revised recommendation in SSR2 Recommendation 9.3.
ICANN Org	18.1	ICANN org should have compliance activities audited externally and hold them to a high standard.	ICANN org encourages the SSR2 RT to clarify the identified issues or risks, how the recommended solution will address them, the expected impact of implementation, and what relevant metrics could be applied to assess implementation. Particularly, ICANN org seeks clarification on the following: ● Who does the SSR2 RT envision conducting the external audit? ● What would the criteria be for an external audit and how would the criteria be applied? ● What is a “high” standard? Who determines that and how is it measured? Further, ICANN org notes that the RDS-WHOIS2 Review Team reviewed ICANN Contractual Compliance activities (see RDS-WHOIS2 Review Final Report) and made a number of recommendations. The Board took action on the RDS-WHOIS2 recommendations in February 2020 (see RDS-WHOIS2 Recommendations, CC.3 - approved, R4.1 and R4.2 - placed in pending status).	This section has been heavily revised and clarified. Please see the revised recommendations in Section E. Contracts, Compliance, and Transparency around DNS Abuse.

Source	SSR2 Section or Rec	Report Section	Comment	Response
M3AAWG	18.2	The ICANN Board should empower the Compliance Office to react to complaints and require Compliance to initiate investigations and enforce contractual obligations against those aiding and abetting systemic abuse, as defined by the SLA. This additional authority could include support for step by step actions around the escalation of enforcement measures and appropriate implementable actions that ICANN org can use in response to any failures to remedy compliance violations within specified timeframes.	(2) Empower ICANN Compliance with contracts and enforcement tools to mitigate domain abuse.	Thank you. Please see SSR2 Recommendation 9.4.
RrSG	18.2	The ICANN Board should empower the Compliance Office to react to complaints and require Compliance to initiate investigations and enforce contractual obligations against those aiding and abetting systemic abuse, as defined by the SLA. This additional authority could include support for step by step actions around the escalation of enforcement measures and appropriate implementable actions that ICANN org can use in response to any failures to remedy compliance violations within specified timeframes.	For recommendation 18.2, the RrSG notes that these obligations exist in the RAA and Compliance already monitors it.	The SSR2 Review Team observed that these obligations are not being met effectively. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16 for revised text.

Source	SSR2 Section or Rec	Report Section	Comment	Response
ICANN Org	18.2	SSR2 Recommendation 18.2: “as defined by the SLA”	Requests for clarification of terms	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
ICANN Org	18.2	The ICANN Board should empower the Compliance Office to react to complaints and require Compliance to initiate investigations and enforce contractual obligations against those aiding and abetting systemic abuse, as defined by the SLA. This additional authority could include support for step by step actions around the escalation of enforcement measures and appropriate implementable actions that ICANN org can use in response to any failures to remedy compliance violations within specified timeframes.	ICANN org notes the ICANN Contractual Compliance team does react to complaints and enforces the contractual obligations in the RA and the RAA. ICANN org seeks clarification on what the SSR2 RT means by “systemic abuse,” and the definition used by the SSR2 RT, as well as the meaning of “aiding and abetting” in the context of the recommendation provided by the SSR2 RT. ICANN org would also request clarification regarding which SLA the SSR2 RT is referring to, and why the SSR2 RT feels that this SLA is appropriate in this context.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
RrSG	18.3	The ICANN Compliance Office should, as their default, involve SLAs on enforcement and reporting, clear and efficient processes, a fully informed complainant, measurable satisfaction, and maximum public disclosure.	For recommendation 18.3, ICANN Compliance already does this (see https://features.icann.org/compliance/dashboard/report-list).	While ICANN Compliance has a dashboard for complaints, it is not clear the extent to which SSR issues are handled within the compliance process. Please see SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties and SSR2 Recommendation 9: Monitor and Enforce Compliance for the SSR2 recommendations that expands upon the original SSR1 recommendation.

Source	SSR2 Section or Rec	Report Section	Comment	Response
ICANN Org	18.3	The ICANN Compliance Office should, as their default, involve SLAs on enforcement and reporting, clear and efficient processes, a fully informed complainant, measurable satisfaction, and maximum public disclosure.	ICANN Contractual Compliance strives to have clear and efficient processes and keep those who make complaints informed and satisfied. If SSR2 RT has data indicating Compliance has not met those goals, ICANN org encourages the SSR2 RT to present the data and develop recommendations that clearly identify ways in which it believes Compliance can better perform their functions to address the deficiencies documented in that data. It is unclear what SLAs SSR2 RT is referring to and with whom those service level agreements would be made. With regards to "maximum public disclosure," ICANN org suggests it would be helpful for the SSR2 RT to document what information should be disclosed, particularly in light of GDPR-related privacy requirements, to whom, and by what means?	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
BC	19	Update Handling of Abusive Naming	The BC concurs with this recommendation. ICANN Org should acknowledge and track the rise of misleading naming and trademark infringement as a growing trend in abusive naming. It has long been recognized that most trademark infringement targets users of famous brands and defrauds the individual user, not the large global brand. Abusers recognize the ease with which they can utilize the goodwill of a brand to lead the user to trust the infringer and provide personal information or funds to the abuser.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
SSAC	19	Update Handling of Abusive Naming	(3.3.14) The rationale that reducing the potential for name similarity contributes to improved security of the DNS can be countered by the desire to express names meaningful to humans in the DNS in the languages, scripts and glyphs that humans use. There is a tension here between utility and security that the report does not cover in sufficient depth. SSAC notes that Recommendations 19's consideration to 'update handling of abusive naming' may be an inappropriate designation of responsibility. ... These recommendations would benefit from an assessment of what falls under ICANN org's remit to enforce, and what efforts ICANN org may be able to facilitate to support a broader community of interest.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
WIPO	19	Update Handling of Abusive Naming	Using so-called homograph spoofing, cybersquatters sometimes take advantage of visual similarity between character sets. ICANN may wish to explore technical (if not contractual) means to enforce the prohibition on the registration of mixed-script domain names combining ASCII with non-ASCII characters which do not minimize user confusion.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
RySG	19	Update Handling of Abusive Naming	The RySG believes that this recommendation is outside the scope of SSR2 and does not support it.	The SSR2 RT received positive feedback from those who would benefit from its implementation, and negative feedback from those who would have to fund its implementation.The SSR2 RT continues to support this recommndation. Clarifications have been added, however. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.

Source	SSR2 Section or Rec	Report Section	Comment	Response
IPC	19		The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below. The IPC strongly supports the RT's recommendations that address investigating and responding to DNS abuse, including Recommendation 12: "Create Legal and Appropriate Access Mechanisms to WHOIS Data," SSR2 Recommendation 13: "Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program (DAAR)," SSR2 Recommendation 17: "Establish a Central Abuse Report Portal," and SSR2 Recommendation 19: "Update Handling of Abusive Naming." ... The IPC also strongly supports and commends the RT's Recommendation 19 to target abusive naming in the DNS. Cybercriminals are assisted in their attacks on individuals and companies through use of misleading names, oftentimes channeling a trusted or well-known name (including in many cases a trademark), to gain the trust of their victims. The IPC encourages ICANN to adopt this recommendation and take steps to make it more difficult for a cybercriminal to take advantage of abusively misleading names.	Thank you. Please see the revised recommendations in Section E. Contracts, Compliance, and Transparency around DNS Abuse, in particular SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties, SSR2 Recommendation 9: Monitor and Enforce Compliance, SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms, SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting, SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements, and SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements.
RrSG	19.1	ICANN org should build upon the current activities to investigate typical misleading naming, in cooperation with researchers and stakeholders, wherever applicable	Recommendation 19.1 is something that is already shared among commercial and community-driven threat exchanges and are used by many companies for their endpoint protection. It is not for ICANN to aggregate and provide these services for free (as some of them are available for purchase)	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
ICANN Org	19.1	SSR2 Recommendation 19.1: "misleading naming"	Requests for clarification of terms	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
RrSG	19.2	When misleading naming rises to the level of abusive naming, ICANN org should include this type of abuse in their DAAR reporting and develop policies and mitigation best practices.	Recommendation 19.2 is not clear. If a misleading domain names become abusive, then it will be listed in the feeds DAAR uses automatically.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
ICANN Org	19.2	SSR2 Recommendation 19.2: "misleading naming" and "abusive naming"	Requests for clarification of terms	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.

Source	SSR2 Section or Rec	Report Section	Comment	Response
ICANN Org	19.2	When misleading naming rises to the level of abusive naming, ICANN org should include this type of abuse in their DAAR reporting and develop policies and mitigation best practices.	Without clear definitions of “misleading” and/or “abusive”, it is difficult to identify bestpractices for mitigation and establish criteria that distinguishes between the two. ICANN org notes ongoing discussions related to the definition of “DNS abuse”. However, we are unaware of any consensus within the community on the definition of “misleading”. Beyond this, ICANN org notes that in order for an abuse type to be included in DAAR, ICANN org needs a public reputation feed that meets the documented OCTO curation criteria1. ICANN org encourages the SSR2 RT to suggest such a feed for what it considers "misleading" and "abusive" naming to be. Further, ICANN org cannot unilaterally develop policy. ICANN org suggests that the SSR2 RT consider directing this element of the recommendation to the Generic Names Supporting Organization (GNSO) Council for review as to whether the recommendation should be considered in a consensus policy development process. See also the ICANN Board comment pertaining to draft recommendations outside of the Board’s oversight responsibilities.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
IPC	19.2		The IPC understand the DAAR to be a collection of existing, publicly available feeds. The IPC suggests that this recommendation might better be expressed as “ICANN Org should seek to identify and incorporate feed (s) tracking this type of abuse in the DAAR. We would also encourage ICANN org to include information covering cybersquatting within the meaning of “abusive naming” for purposes of reporting and other requirements around anti-abuse measures, to the extent this category is not already explicitly covered.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
RrSG	19.3	ICANN org should publish the number of abusive naming complaints made at the portal in a form that allows independent third parties to analyze, mitigate, and prevent harm from the use of such domain names.	For recommendation 19.3, such data needs to be curated and require a Traffic Light Protocol for sharing such information. Furthermore, this requires a clear definition of what is misleading and what can lead to abuse.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
RrSG	19.4	ICANN org should update the current "Guidelines for the Implementation of IDNs" [citation to be added] to include a section on names containing trademarks, TLD-chaining, and the use of (hard-to-spot) typos. Furthermore, ICANN should contractually enforce "Guidelines for the Implementation of IDNs" for gTLDS and recommend that ccTLDs do the same.	Recommendation 19.4 should originate from a PDP rather than a review team. Additionally, it is not the place of a review team to initiate RAA or RA negotiation or changes.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.

Source	SSR2 Section or Rec	Report Section	Comment	Response
RySG	19.4	ICANN org should update the current "Guidelines for the Implementation of IDNs" [citation to be added] to include a section on names containing trademarks, TLD-chaining, and the use of (hard-to-spot) typos. Furthermore, ICANN should contractually enforce "Guidelines for the Implementation of IDNs" for gTLDS and recommend that ccTLDs do the same.	The ICANN IDN Guidelines should not duplicate, potentially putting itself in conflict with the Registry Agreement or ICANN policies, what otherwise can be applied in a more general way to all types of domain names, ASCII and IDN. For example, Specification 7 (Rights Protection Mechanisms) of the 2017 Base Registry Agreement applies equally to all domain name registration regardless of the script used. Further, there seems to be the incorrect perception that ICANN does not enforce the IDN Implementation Guidelines upon gTLD registries, when the opposite is true. ICANN uses the Registry System Testing process to evaluate registry operator's implementation of the IETF Standards and IDN Guidelines (i.e. Specification 6 of the 2017 Base Registry Agreement), prior to delegation and when required by a new Registry Service Evaluation Process. If the registry operator does not meet the requirement as set forth in their registry agreement, then the registry operator needs to remediate the issues before ICANN approves any registry service.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
IPC	19.4		The IPC encourages the RT to expand on this recommendation, which presently lacks clarity and specificity. The recommendation might include specific reference to cybersquatting and the use of IDN homoglyphs to mimic trademarks as an example of abusive naming through IDNs.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
BC	20	Complete Development of a DNS Regression Testing	The BC concurs with this recommendation.	Thank you. Please see the updated text in SSR2 Recommendation 19: Complete Development of the DNS Regression Test Suite
RSSAC	20	Complete Development of a DNS Regression Testing	The RSSAC limits its comments to its remit (i.e., the recommendations on Key Signing Key rollover, root server operations). With that in mind, the RSSAC supports the following SSR2 recommendations: [20, 21, 22]	Thank you. Please see the updated text in SSR2 Recommendation 19: Complete Development of the DNS Regression Test Suite and SSR2 Recommendation 20: Formal Procedures for Key Rollovers. The original SSR2 Recommendation 22 has been removed from the report.
RrSG	20	Complete Development of a DNS Regression Testing	It is not clear how this recommendation will be paid for, and what the benefit is over other commercially available solutions.	SSR2 is not proposing a way to fund the implementation. Other approaches do not provide publicly available interoperabilty information. Please see the updated text in SSR2 Recommendation 19: Complete Development of the DNS Regression Test Suite
ICANN Org	20	Complete Development of a DNS Regression Testing	However, in reading Recommendations 20.1 and 20.2, ICANN org is unsure about the scope of such testing. Regression test suites are never really "complete" as they must always be added to as new issues are identified, and their mitigations deployed. Further, while OCTO has done work in the resolver testbed to test a sampling of open source resolvers, this can in no way be considered complete or even representative of all resolvers that are in use on the Internet today. Finally, the text of 20.3 indicates ICANN org should develop a suite for "DNS regression testing," but (counter to the "Rationale and Findings" of that recommendation which mentions "resolver behavior") does not limit the functionality to regression test, i.e., it can be read that org should develop a regression test suite for authoritative servers, resolvers, forwarders, etc. ICANN org asks the SSR2 RT to clarify the intent of this recommendation based on the comments above.	Thank you for helping the SSR2 RT improve this recommendation. Please see the updated text in SSR2 Recommendation 19: Complete Development of the DNS Regression Test Suite.
IPC	20		The IPC is supportive of this recommendation.	Thank you. Please see the updated text in SSR2 Recommendation 19: Complete Development of the DNS Regression Test Suite.

Source	SSR2 Section or Rec	Report Section	Comment	Response
SSAC	20.1	ICANN org should complete the development of a suite for DNS regression testing.	(3.3.15) It is useful to understand how various available implementations of DNS name services operate, but it must be remembered that almost any collection of DNS software would by no means include the entirety of the DNS service environment. There are no well understood means of measuring how many end users and services use any particular software bundle, directly or indirectly.	Thank you for helping the SSR2 RT improve this recommendation. Please see the updated text in SSR2 Recommendation 19: Complete Development of the DNS Regression Test Suite.
SSAC	20.2	ICANN org should ensure that the capability to perform functional testing of different configurations and software versions is implemented and maintained	(3.3.16) It is suggested that the recommendation be revised to recognise the existing activity and to include some proposed measurable outcomes.	Thank you for helping the SSR2 RT improve this recommendation. Please see the updated text in SSR2 Recommendation 19: Complete Development of the DNS Regression Test Suite.
BC	21	Implement the Recommendations from SAC063 and SAC073 and Establish Formal Procedures for Key Rollovers	The BC concurs with this recommendation.	Thank you. Please see the updated text in SSR2 Recommendation 20: Formal Procedures for Key Rollovers.
RSSAC	21	Implement the Recommendations from SAC063 and SAC073 and Establish Formal Procedures for Key Rollovers	The RSSAC limits its comments to its remit (i.e., the recommendations on Key Signing Key rollover, root server operations). With that in mind, the RSSAC supports the following SSR2 recommendations: [20, 21, 22]	Thank you. Please see the updated text in SSR2 Recommendation 19: Complete Development of the DNS Regression Test Suite and SSR2 Recommendation 20: Formal Procedures for Key Rollovers. The original SSR2 Recommendation 22 has been removed from the report.
SSAC	21	“The review team found no evidence that the propagation delay between publication to each of the letters, and then to each of a letter’s instances, is well understood. Propagation delay is (for example) a relevant aspect of ensuring that validating resolvers are able to retrieve the same DNSKEY RRset, and rollover timing can be predictable.”	(3.3.17) The interactions of DNS resolvers with respect to multiple instances of authoritative data, and the interactions with cached data held in various recursive resolvers are appreciated in the design of the KSK role. The report’s assertion relating to propagation delay is technically fallacious in this context.	The finding underscores a lack of evidence and the text hs been updated to request publication and incorporation of such evidence. Please see the updated text in Section F.4.a. Key Rollover and SSR2 Recommendation 20: Formal Procedures for Key Rollovers.
SSAC	21	“Software and systems process analysis is a research branch of computer science’s software engineering ...”	(3.3.18) Some SSAC reviewers suggest that this paragraph, and the preceding paragraph beginning with, "For example, the global DNS Root .." should be deleted from the draft SSR2 report.	Please see the updated text in Section F.4.a. Key Rollover and SSR2 Recommendation 20: Formal Procedures for Key Rollovers.

Source	SSR2 Section or Rec	Report Section	Comment	Response
RrSG	21	Implement the Recommendations from SAC063 and SAC073 and Establish Formal Procedures for Key Rollovers	The RrSG does not have a position on this recommendation.	Thank you.
ICANN Org	21	Implement the Recommendations from SAC063 and SAC073 and Establish Formal Procedures for Key Rollovers	ICANN org notes that all advice to the Board is processed via a defined process. ICANN org tracks the implementation of this advice via the Action Request Register (ARR). ICANN org notes that recommendations from any review team cannot circumvent this process and suggests that the SSR2 RT track the status of this advice as it continues to deliberate on Recommendation 21. ICANN org notes that on 15 October 2018, ICANN org determined that the first-ever changing of the cryptographic key that helps protect the DNS was completed with minimal disruption of the global Internet. The communication plan, test pass, and data collection program are all part of the overall KSK Rollover Project, which were established and extensively vetted with the DNS technical community.	Please see the updated text in Section F.4.a. Key Rollover and SSR2 Recommendation 20: Formal Procedures for Key Rollovers.
IPC	21		The IPC is supportive of this recommendation.	Thank you. Please see the updated text in SSR2 Recommendation 20: Formal Procedures for Key Rollovers.
SSAC	21.1	ICANN org should implement the recommendations from SAC063 and SAC073 in order to ensure the SSR of the KSK rollover process.	(3.3.19) The SSAC suggests removing this recommendation in its entirety.	This recommendation has been removed.

Source	SSR2 Section or Rec	Report Section	Comment	Response
SSAC	21.2	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, FSM) for public comment, and community feedback should be incorporated. 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 lessons learned can be used to adjust the process.	(3.3.20) Some SSAC reviewers believe that this recommendation is simply not implementable in the context of the DNS and the KSK roll. In many other system contexts, such a generic recommendation might have some relevance, but not in the DNS. There are no clear and authoritative means of measuring DNS name resolution and validation and no way of defining either acceptance criteria nor failure thresholds. Some SSAC reviewers have suggested that the SSR2 RT should clarify what work currently underway by ICANN org is not meeting their expectations and identify what work needs to be expanded upon or retooled.	The review team disagrees. Work has been done to use this approach in medical processes, and election security. The text has been augmented with greater description, peer-reviewed citations, and more description of the matter. Please see the updated text in Section F.4.a. Key Rollover and SSR2 Recommendation 20: Formal Procedures for Key Rollovers.
SSAC	21.3	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.	(3.3.21) While this recommendation may be useful, it should not be considered a high priority.	The SSR2 Review Team has modified the priority of this recommendation to "Medium." Please see SSR2 Recommendation 20: Formal Procedures for Key Rollovers for the revised text.
BC	22	Establish Baseline Security Practices for Root Server Operators and Operations	The BC concurs with this recommendation.	This recommendation has been removed.
RSSAC	22	Establish Baseline Security Practices for Root Server Operators and Operations	The RSSAC limits its comments to its remit (i.e., the recommendations on Key Signing Key rollover, root server operations). With that in mind, the RSSAC supports the following SSR2 recommendations: [20, 21, 22]	This recommendation has been removed.

Source	SSR2 Section or Rec	Report Section	Comment	Response
SSAC	22	Establish Baseline Security Practices for Root Server Operators and Operations	(3.3.22) ICANN, as an important stakeholder in the DNS root server framework is certainly capable of advocating a particular stance and this report may well recommend such a position of advocacy, but that position falls short of any enforcement capability. The principles espoused in recommendations 22.1 and 22.1 are sound, but their manner of implementation by ICANN should reflect the realities of the at-a-distance relationship between the root server operators and ICANN.	This recommendation has been removed.
RrSG	22	Establish Baseline Security Practices for Root Server Operators and Operations	The RrSG does not have a position on this recommendation.	This recommendation has been removed.
IPC	22		The IPC is supportive of this recommendation.	This recommendation has been removed.
ICANN Org	22.1	ICANN org, in close cooperation with RSSAC and other relevant stakeholders, should ensure that the RSS governance model as proposed by RSSAC037 includes baseline security best practices for root server operators and operations in order to minimize the SSR risks associated with root server operation. These best practices should include change management, verification procedures, and sanity check procedures.	It is ICANN org's understanding that the Governance Working Group (GWG), as defined in RSSAC037, is in the early stages of formation. If the GWG requests assistance from ICANN org in identifying or making available security best practices, we would certainly do so as part of our already existing support for the GWG.	This recommendation has been removed.
ICANN Org	22.2	ICANN org should also develop relevant KPIs to measure the implementation of these best practices and requirements and ensure yearly public reporting on how Root Server Operators (RSOs) and other relevant parties, including ICANN org, can meet these KPIs.	ICANN org feels that development of Key Performance Indicators (KPIs) to measure root server security best practices should be led by Root Server System Advisory Committee (RSSAC), the GWG, and/or the root server operators themselves. It is worth reiterating that ICANN org cannot force the root server operator community to abide by best practices. While it is feasible that ICANN org could ensure yearly public reporting on (publicly published) KPIs, it is unclear what value such reporting would bring. With that said, ICANN org would certainly assist in the development of KPIs and reporting on those KPIs as part of our ongoing support of RSSAC and the GWG if directed by the Board as a result of advice by RSSAC or requested by the GWG.	This recommendation has been removed.

Source	SSR2 Section or Rec	Report Section	Comment	Response
SSAC	22.3	ICANN org should document hardening strategies of the ICANN Managed Root Server (IMRS), commonly known as L-Root, and should encourage other RSOs to do the same.	(3.3.23) This recommendation refers to a “hardening strategy” that is not explained in the draft report.	This recommendation has been removed.
ICANN Org	22.3	ICANN org should document hardening strategies of the ICANN Managed Root Server (IMRS), commonly known as L-Root, and should encourage other RSOs to do the same.	It is unclear what problem this recommendation is trying to solve. Does SSR2 RT believe that IMRS or the other RSOs, either individually or collectively, have insecure infrastructure? Given that documented hardening strategies can provide a “roadmap” to attackers, i.e., identifying weaknesses based on the documented hardening strategy, ICANN org does not feel publishing the strategy we have used to protect IMRS would contribute positively to IMRS security, stability, and resiliency. However, ICANN org does share information with the other RSOs on both operational and security aspects (following FIRST's Traffic Light Protocol).	This recommendation has been removed.
ICANN Org	22.4	ICANN org should ensure that the IMRS uses a vulnerability disclosure process (not necessarily public), security reports and intelligence, and communication with researchers and RSSAC advice or recommendations, where applicable.	ICANN org has an incident vulnerability disclosure process through the Security and Network Engineering (SaNE) group which operates IMRS. This group is also responsible for ICANN org’s digital security. The ICANN org incident disclosure process is therefore applied to the IMRS. Because OCTO defines IMRS strategy and provides and tracks research, including SSR-related research, ICANN org will continue to ensure the SaNE group makes use of the resources available to it. ICANN org encourages the SSR2 RT to consider this work to determine if it addresses the identified issue/risk. If the SSR2 RT’s intent is to recommend implementation of something beyond what has already been implemented, ICANN org encourages the SSR2 RT to clarify what issues or risks exist from the current operational model, how the SSR2 RT recommendations will address them, and what relevant metrics could be applied to assess implementation.	This recommendation has been removed.
BC	23	Accelerate the Implementation of the New-Generation RZMS	The BC concurs with this recommendation.	Thank you. Please see SSR2 Recommendation 21: Improve the Security of Communications with TLD Operators for revised text.
SSAC	23	Accelerate the Implementation of the New-Generation RZMS	(3.3.24) There are many reasons why secure systems take time to develop and test. Identifying vulnerabilities in any system takes time and careful analysis. The task of assuring the end client of a secure system that the system is indeed adequately robust and secure requires a comprehensive phase of analysis. It is unclear why this report is recommending that the process be “accelerated”. What issue or issues are being addressed by hastening this particular development? The report does not clearly explain why this acceleration is necessary	The proposed recommendation does not refer to the security of the root zone management system, but to the communication with TLD operators that are now done by sending clear text emails and access to the system by using the user/password combination. Encrypted email exchange and multi-factor authentication, in our opinion, do not require extensive analysis and expertise to be implemented in the existing system and later used in the new RZMS system. The fact that there has been no abuse of these security vulnerabilities does not mean that they are not possible in the future. Please see SSR2 Recommendation 21: Improve the Security of Communications with TLD Operators for clarified text to this recommendation.
RrSG	23	Accelerate the Implementation of the New-Generation RZMS	The RrSG does not have a position on this recommendation.	Thank you.
IPC	23		The IPC is supportive of this recommendation.	Thank you. Please see SSR2 Recommendation 21: Improve the Security of Communications with TLD Operators for revised text.

Source	SSR2 Section or Rec	Report Section	Comment	Response
ICANN Org	23.2	ICANN org should launch public comment as soon as possible on changes regarding revisions to the RZMS policies.	... ICANN org requests that the SSR2 RT clarify if it intends this recommendation to require a public comment proceeding whenever IANA makes changes to the RZMS.	The text of this recommendation has been clarified; please see SSR2 Recommendation 21: Improve the Security of Communications with TLD Operators for revised text.
BC	24	Create a List of Statistics and Metrics Around the Operational Status of the Unique Identifier Systems	The BC concurs with this recommendation.	Thank you. Please see SSR2 Recommendation 22: Service Measurements for revised text.
RrSG	24	Create a List of Statistics and Metrics Around the Operational Status of the Unique Identifier Systems	If this recommendation is restricted to the ennumerated items in 24.1, then the RrSG supports this recommendation. If this recommendation is intended to include registrars and registries, then it is not acceptable. As indicated elsewhere, it is not ICANN's role to publicly score the "operational status" of contracted parties.	The language for this recommendation has been clarified to indicate it applies only to those services ICANN org has authoritative purview over. Please see SSR2 Recommendation 22: Service Measurements for revised text.
IPC	24		The IPC is supportive of this recommendation.	Thank you. Please see SSR2 Recommendation 22: Service Measurements for revised text.
SSAC	24.1	ICANN org should create a list of statistics and metrics that reflect the operational status (such as availability and responsiveness) of each type of unique identifier information, such as root-zone related service, IANA registries, and any gTLD service that ICANN org has authoritative purview over.	(3.3.26) The term “of each type of unique identifier information” is used and specific mention is made of “IANA Registries.” The scope of this recommendation apparently includes the IETF Protocol Parameter Registry function. Should the agency for whom the function is being performed, namely the IETF, perform a review of ICANN’s performance of execution of the roles described by the Memorandum of Understanding (MoU) between ICANN and the IETF?	The language for this recommendation has been clarified to indicate it applies to the availability of the services themselves, not the response times of IANA. Please see SSR2 Recommendation 22: Service Measurements for revised text.
ICANN Org	24.1	ICANN org should create a list of statistics and metrics that reflect the operational status (such as availability and responsiveness) of each type of unique identifier information, such as root-zone related service, IANA registries, and any gTLD service that ICANN org has authoritative purview over.	ICANN org notes that IANA already measures service availability of its critical services as a component of its various SLAs under the IANA contracts. IANA maintains around 3000 registries, mostly served on common architecture that would have the same operational status. ICANN org encourages the SSR2 RT to consider in its final recommendation if operational status could be grouped by service type and not by unique identifier type.	The language for this recommendation has been clarified to indicate it applies to the availability of the services themselves, not the response times of IANA. Please see SSR2 Recommendation 22: Service Measurements for revised text.
BC	25	Ensure the Centralized Zone File Data Access is Consistently Available	The BC concurs with this recommendation.	Thank you. Please see the revised rationale in Section E.2.b.ii.Centralized Zone Data Service and the SSR2 Recommendation 11: Resolve CZDS Data Access Problems.

Source	SSR2 Section or Rec	Report Section	Comment	Response
RrSG	25	Ensure the Centralized Zone File Data Access is Consistently Available	The RrSG requires additional information, as it is not clear what the concern this recommendation intends to address. Additionally, the term "other data" is very broad and should be narrowed.	Thank you. Please see the revised rationale in Section E.2.b.ii.Centralized Zone Data Service and the SSR2 Recommendation 11: Resolve CZDS Data Access Problems.
IPC	25		The IPC is supportive of this recommendation, subject to above-noted concerns about CZDS access, and particularly the treatment of Brand TLDs.	Thank you. The review team has taken this comment into consideration. Please see the revised text in E.2.b.ii. Centralized Zone Data Service.
ICANN Org	25.1	The ICANN community and ICANN org should take steps to ensure that access to CZDS as well as other data is available, in a timely manner, and without unnecessary hurdles to requesters.	ICANN org encourages the SSR2 RT to provide examples of “unnecessary hurdles” that requesters are experiencing. ...	Thank you. Please see the revised rationale in Section E.2.b.ii.Centralized Zone Data Service and the SSR2 Recommendation 11: Resolve CZDS Data Access Problems.
RySG	25.1	The ICANN community and ICANN org should take steps to ensure that access to CZDS as well as other data is available, in a timely manner, and without unnecessary hurdles to requesters.	The RySG notes that the current CZDS structure, which currently satisfies the recommendation, was arrived at after much negotiation taking into account the varying concerns of the ICANN community. This negotiated solution should not be overruled by a stroke of the Board’s pen.	The SSR2 Review Team respectfully notes that if CZDS is failing to achieve its stated goals, it is within the purview of ICANN org and Board to take action. Please see the revised rationale in Section E.2.b.ii.Centralized Zone Data Service and the SSR2 Recommendation 11: Resolve CZDS Data Access Problems.
SSAC	25.2	ICANN org should implement the four recommendations in SSAC 97	(3.3.27) This again raises the same issue of quoting recommendations from other ICANN supporting organisations and advisory committees. If the reason to reproduce these recommendations in the SSR2 report is because the SSR2 RT has concluded that the ICANN board is not paying due attention to its advisory bodies then it should say so directly. If this is not the case, then what purpose is served by reproducing these recommendations here?	This recommendation has been removed.
ICANN Org	25.2	ICANN org should implement the four recommendations in SSAC 97.	ICANN org notes that on 23 June 2018, the Board accepted the advice in SAC097 and directed the ICANN President and CEO or his designee to implement the recommendations contained in SAC097. ICANN org tracks the implementation of this advice via the Action Request Register (ARR) and suggests that the SSR2 RT may wish to consider the status of this advice as it continues to deliberate on Recommendation 25.2.	This recommendation has been removed.
RySG	25.2	ICANN org should implement the four recommendations in SSAC 97.	The RySG notes that the four recommendations flagged by the SSR2 have already been accepted by the ICANN Board according to this Board resolution https://www.icann.org/resources/board-material/resolutions-2018-06-23-en#1.g. The Board has already directed ICANN org to implement these recommendations, so there is no need for the SSR2 to include a recommendation that says the very same thing. This should not be included in the Final Report.	This recommendation has been removed.
BC	26	Document, Improve, and Test the EBERO Processes	The BC concurs with this recommendation.	Thank you. Please see SSR2 Recommendation 24: Improve Transparency and End-to-End Testing for the EBERO Process for revised text.

Source	SSR2 Section or Rec	Report Section	Comment	Response
NCSG	26	Document, Improve, and Test the EBERO Processes	#Recommendation 26: urges ICANN to take exemplary actions to conduct testings related to the Emergency Back-End Registry Operator (EBERO) processes. This is vital for the resiliency and stability of the DNS operations. We require the review team to add more measurable actions items to this recommendation. Those should include progression state and deadlines, for instance, 50% of the testing be completed within 5 years, each domain should be tested every 5 years, etc.	The aim of the tests is not to examine each TLD individually but to check and train the procedure and readiness of each entity involved in the process. ICANN should, within its responsibilities, propose measurable action items. They should include datasets used for testing, progression state and deadlines. Please see Section F. 5. Emergency Back-End Registry Operator (EBERO) and SSR2 Recommendation 24: Improve Transparency and End-to-End Testing for the EBERO Process for revised text.
RrSG	26	Document, Improve, and Test the EBERO Processes	The RrSG does not have a position on this recommendation.	Thank you. Please see SSR2 Recommendation 24: Improve Transparency and End-to-End Testing for the EBERO Process for revised text.
IPC	26		The IPC is supportive of this recommendation.	Thank you. Please see SSR2 Recommendation 24: Improve Transparency and End-to-End Testing for the EBERO Process for revised text.
ICANN Org	26.1	ICANN org should publicly document the ERERO processes, including decision points, actions, and exceptions. The document should describe the dependencies for every decision, action, and exception.	ICANN org requests the SSR2 to provide more specific language as to what kind of information regarding decisions and dependencies should be made available to help document the EBERO processes. For example, is the SSR2 requesting the publication of process/procedure documentation, diagrams, flowcharts, FAQs, etc. for how an EBERO event is declared?	The review team requests publication of documents that describe process / procedure, diagrams and flowcharts. That should also include clear definition of decision points and events on when and how an EBERO event is declared. Please see SSR2 Recommendation 24.1 for the revised and clarified text.
SSAC	26.3	ICANN org should publicly conduct EBERO smoke-testing at predetermined intervals using a test plan coordinated with the ICANN contracted parties in advance to ensure that all exception legs are exercised and publish the results.	(3.3.28) This recommendation refers to “smoke-testing”. The term is not explained in the draft report.	This term has been replaced with "testing" in the recommendation. Please see SSR2 Recommendation 24: Improve Transparency and End-to-End Testing for the EBERO Process for revised text.
ICANN Org	26.3	SSR2 Recommendation 26.3: “smoke testing”	Requests for clarification of terms	This term has been replaced with "testing" in the recommendation. Please see SSR2 Recommendation 24: Improve Transparency and End-to-End Testing for the EBERO Process for revised text.
ICANN Org	26.4	ICANN org should improve the process by allowing the gTLD Data Escrow Agent to send the data escrow deposit directly to the EBERO provider	ICANN org requests clarification as to what issues or risks the SSR2 RT intends to address with this recommendation. Further, ICANN org notes that there is no contractual relationship between the EBEROs and the Data Escrow Agents (DEAs) of the gTLDs and while allowing an agent to release escrow file(s) directly to an EBERO provider may remove a process step, it may also add additional complexity (i.e., with maintenance, testing, contracts and costs) because of the need for a new mechanism to release the file(s).	The review team has clarified the language of this recommendation; please see SSR2 Recommendation 24.1.
BC	27	Update the DPS and Build Consensus Around future DNSKEY Algorithm Rollovers	The BC concurs with this recommendation.	Thank you. Please see SSR2 Recommendation 23: Algorithm Rollover for revised language for this recommendation.

Source	SSR2 Section or Rec	Report Section	Comment	Response
Loganaden Velvindron	27	Cryptography "Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC" (RFC 6605) has been published by the IETF to specify the use of ECDSA with curve P-256 and SHA-256 in DNSSEC. "	I am wondering why https://tools.ietf.org/html/rfc8080 is not mentioned on page 51 ? Is there an issue with EdDSA for DNSSEC ?	There is no issue with edDSA for DNSSEC. The report now talks about Elliptic Curve Cryptography (ECC) to include ECDSA as well as EdDSA. Please see SSR2 Recommendation 23: Algorithm Rollover and Appendix F: Research Data on Cryptography for revised text.
SSAC	27	Update the DPS and Build Consensus Around future DNSKEY Algorithm Rollovers	(3.4.1) The discussion on cryptography notes that: “Recent guidance from the US National Security Agency recommends using 3072 bits for RSA. ECDSA [Elliptic Curve Digital Signature Algorithm] seems to offer a better alternative than very large RSA keys”. The reference listed has specific nuances in an National Security System (NSS) context but would necessarily not apply to DNSSEC. While recommendation 27.1 is general and sufficient as a recommendation, the rationale is too prescriptive.	This has been moved to a supporting research section in Appendix F: Research Data on Cryptography. Please see SSR2 Recommendation 23: Algorithm Rollover for revised text to the recommendation itself.
RrSG	27	Update the DPS and Build Consensus Around future DNSKEY Algorithm Rollovers	The RrSG does not have a position on this recommendation.	Thank you.
IPC	27		The IPC is supportive of this recommendation.	Thank you. Please see SSR2 Recommendation 23: Algorithm Rollover for revised language for this recommendation.
NCSG	27		We mostly agree with all the recommendations made within this section. Here also, as a reminder, there is a citation left to be added (page 51 of the draft report).	Thank you. All citations have been updated in the report.
SSAC	27.1	PTI operations should update the DPS to facilitate the transition from one digital signature algorithm to another, including an anticipated transition from the RSA digital signature algorithm to ECDSA or to future post-quantum algorithms, which will create a more resilient DNS while providing the same or greater security.	(3.4.2) The SSAC agrees with the recommendation that the DPS should provide explicit mention of the possibility of a transition from one digital signature to another. The SSAC believes that the explicit references to ECDSA and post-quantum algorithms are unnecessary in this recommendation. The expectation that any such algorithm changes will not degrade security is a prudent expectation, but this recommended action to revise the DPS should remain more generic in nature.	This has been moved to a supporting research section in Appendix F: Research Data on Cryptography. Please see SSR2 Recommendation 23: Algorithm Rollover for revised text to the recommendation itself.

Source	SSR2 Section or Rec	Report Section	Comment	Response
ICANN Org	27.1	PTI operations should update the DPS to facilitate the transition from one digital signature algorithm to another, including an anticipated transition from the RSA digital signature algorithm to ECDSA or to future post-quantum algorithms, which will create a more resilient DNS while providing the same or greater security.	ICANN org notes that the Root KSK DNSSEC Practice Statement (DPS) is just one component of implementing operational plans around changing digital signature algorithms, and that such a change must be carefully studied and tested. Such changes do not necessarily create a more resilient DNS if impacts are not properly understood before execution, and many risks pertain to elements — like resolver behavior — that are not under the scope of the DPS. ICANN org requests that the SSR2 RT provide a recommendation that more fully elaborates on the essential requirements and \conditions for such an algorithm change to be considered and implemented.	The SSR2 Review Team does not intend to prescribe how the algorithm rollover should be conducted; however, the complexity of the rollover is acknowledged in the revised SSR2 Recommendation 23.2.
SSAC	27.2	As root DNSKEY algorithm rollover is a very complex and sensitive process, PTI operations should work with other root zone partners and the global community to develop a consensus plan for future root DNSKEY algorithm rollovers, taking into consideration the lessons learned from the first root KSK rollover in 2018.	(3.4.3) Accordingly, the SSAC agrees with this recommendation.	Thank you.
ICANN Org	27.2	As root DNSKEY algorithm rollover is a very complex and sensitive process, PTI operations should work with other root zone partners and the global community to develop a consensus plan for future root DNSKEY algorithm rollovers, taking into consideration the lessons learned from the first root KSK rollover in 2018.	ICANN org notes that IANA is consulting with the community on its proposal for how future Root Zone Key Signing Key (KSK) changes will be made. IANA presented this proposal at ICANN66 in Montreal and recently closed a public comment period on it. IANA is reviewing the feedback which will inform the final approach, which will be put into operational practice. ICANN org encourages the SSR2 RT to consider this work as it formulates its final recommendation. Further, ICANN org considers the evaluation of the requirements for a cryptographic algorithm roll to be distinct from evaluating the requirements of future rollovers in general.	The consultation on futher KSK rollover has been acknowledged in Section F.4.a Key Rollover and SSR2 Recommendation 20: Formal Procedures for Key Rollovers. The review team noted that this consultation does not include provisions for an algorithm rollover, and at some point in the future an algorithm transition will need to take place.
BC	28	Develop a Report on the Frequency of Measuring Name Collisions and Propose a Solution	The BC concurs with this recommendation.	Thank you. Please see SSR2 Recommendation 17: Measuring Name Collisions for revised text.

Source	SSR2 Section or Rec	Report Section	Comment	Response
SSAC	28	Develop a Report on the Frequency of Measuring Name Collisions and Propose a Solution	(3.4.4) It is unclear why the topic of “Name Collision” in Workstream 4 falls into this Future Challenges category when the topic seems more like an aspect of the current environment that has been studied for over a decade already and continues to be studied, including as part of the SSAC's Name Collision Analysis Project (NCAP). A more logical place for this section of the report would appear to be within Workstream 3’s Review of the Security, Stability and Resilience of the DNS System.	The text has been revised and clarified, and this section of the document significantly restructured. Please see Section F.1. Name Collisions and SSR2 Recommendation 17: Measuring Name Collisions for revised text and placement.
SSAC	28	Develop a Report on the Frequency of Measuring Name Collisions and Propose a Solution	(3.4.5) It is unclear what is being proposed here. The recommendation title in the summary at the front of the report and the recommendation title in the body of the report differ, although the text of the sub-recommendations match. It is also unclear what is meant by “Propose a Solution”. This section could benefit from more clarity and context on whether ICANN org should be proposing a solution, to whom the proposal should be presented and how that proposed solution relates to the current NCAP study.	The text has been revised and clarified, and this section of the document significantly restructured. Please see Section F.1. Name Collisions and SSR2 Recommendation 17: Measuring Name Collisions for revised text and placement.
RrSG	28	Develop a Report on the Frequency of Measuring Name Collisions and Propose a Solution	The RrSG does not have a position on this recommendation.	Thank you
RySG	28	Develop a Report on the Frequency of Measuring Name Collisions and Propose a Solution	The RySG is unclear how this recommendation overlaps with the ongoing NCAP Studies - it’s possible that the RT is referring to malicious name collisions at the second level, not inadvertent collisions at the top level. The RySG supports independent studies on malicious name collisions.	The text has been revised and clarified, and this section of the document significantly restructured. Please see Section F.1. Name Collisions and SSR2 Recommendation 17: Measuring Name Collisions for revised text and placement.
IPC	28		The IPC is supportive of this recommendation.	Thank you. Please see Section F.1. Name Collisions and SSR2 Recommendation 17: Measuring Name Collisions for revised text and placement.
SSAC	28.1	ICANN org should produce findings that characterize the nature and frequency of name collisions and resulting concerns. The ICANN community should implement a solution before the next round of gTLDs.	(3.4.6) In what way does this recommendation materially differ from the existing NCAP study being undertaken under the auspices of SSAC?	The recommendations of NCAP study, on many occasions, are based on rationale rather than investigations of actual datasets. Moreover, there has to be a way to "characterize the nature" of name collisions. Please see Section F.1. Name Collisions and SSR2 Recommendation 17: Measuring Name Collisions for revised text and placement.

Source	SSR2 Section or Rec	Report Section	Comment	Response
SSAC	28.2	ICANN org should facilitate this process by initiating an independent study of name collisions through to its eventual completion and adopt or account for the implementation or non-adoption of any resulting recommendations. By “independent,” SSR2 RT means that ICANN org should ensure that the SSAC Name Collision Analysis Project (NCAP) work party research and report evaluation team’s results need to be vetted by parties that are free of any financial interest in TLD expansion.	(3.4.7) It is unclear what is being proposed here. Does this recommendation propose the establishment of a new study of name collisions that is to operate in parallel to, but fully independent of, the SSAC NCAP activity? Or is the recommendation proposing a “vetting” of the SSAC NCAP outcomes by some third party or parties that have no financial interest in TLD expansion?	The SSR2 Review Team agrees that the NCAP study is valuable. That study did not, hwoever, address the continued need for mechanisms to discover unreported name collisions, both malicious and accidental. The review team is recommending that ICANN org develop and implement a clear policy for handling New gTLD name collisions. Please see SSR2 Recommendation 17.2.
SSAC	28.3	ICANN org should enable community reporting on instances of name collision. These reports should allow appropriate handling of sensitive data and security threats and should be rolled into community reporting metrics.	(3.4.8) What is the intended objective of this recommendation? How would the reported data be used? To what end? The report fails to adequately motivate this recommendation, lack a clear definition of what is intended by “community reporting,” nor give a clear indication of measurable outcomes. In terms of SMART criteria, this recommendation appears to be lacking in terms of specificity, measurability, and relevance.	This recommendation has been removed.
BC	29	Focus on Privacy and SSR Measurements and Improving Policies Based on Those Measurements	The BC concurs with this recommendation.	Thank you. Please see Section E.4. Privacy and Data Stewardship and SSR2 Recommendation 16: Privacy Requirements and RDS for the revised text.
SSAC	29	Focus on Privacy and SSR Measurements and Improving Policies Based on Those Measurements	(3.4.9) Why is the topic of “Privacy” in Workstream 4 a Future Challenge? This would conventionally be classified as a current topic. Does the SSR2 RT have evidence that ICANN org is not adequately focusing on Privacy and SSR Measurements already? The recommendation implies that the review has taken the position that the level of focus and attention is inadequate, but has not provided any material in the report that substantiates such a conclusion.	The recommendations relating to Privacy have been significantly restructured and moved to a different section of the document. Please see Section E.4. Privacy and Data Stewardship and SSR2 Recommendation 16: Privacy Requirements and RDS.

Source	SSR2 Section or Rec	Report Section	Comment	Response
SSAC	29	Focus on Privacy and SSR Measurements and Improving Policies Based on Those Measurements	(3.4.10) The report notes in the section relating to Rationale and Findings on Privacy, that "ICANN org, in having a privacy policy that covers registration information and having Bylaws that requires it enforce its own policies, is in conflict with their statement that ICANN org is not responsible for data protection and privacy." This is an unusual 17 interpretation of the ICANN statement, in that the disclaimer is about the general state of privacy on the Internet while the org does have a privacy policy relating to data gathered by the org.	The recommendations relating to Privacy have been significantly restructured and moved to a different section of the document. Please see Section E.4. Privacy and Data Stewardship and SSR2 Recommendation 16: Privacy Requirements and RDS.
RySG	29	Focus on Privacy and SSR Measurements and Improving Policies Based on Those Measurements	While the RySG supports ICANN tracking new technology and evolving privacy laws and regulations as part of its overall risk management management, the RySG believes that much of this recommendation is out of scope for SSR2. Specifically, we oppose the creation of specialized compliance officers to micromanage contracted party operations. Registries and registrars are responsible for complying with all local laws - ICANN's compliance team doesn't need to duplicate the function of local law enforcement. The RySG also notes its support for recommendation 31.	The recommendations relating to Privacy have been significantly restructured and moved to a different section of the document. Please see Section E.4. Privacy and Data Stewardship and SSR2 Recommendation 16: Privacy Requirements and RDS.
IPC	29		The IPC is supportive of this recommendation, while noting that the following recommendation is unclear and potentially subject to unintended interpretation in implementation: 'ICANN org's DPO should also be responsible for external DNS PII'.	The recommendations relating to Privacy have been significantly restructured and moved to a different section of the document. Please see Section E.4. Privacy and Data Stewardship and SSR2 Recommendation 16: Privacy Requirements and RDS.
SSAC	29.1	ICANN org should monitor and regularly report on the privacy impact of technologies like DoT (DNS over TLS) and DoH (DNS over HTTPS).	(3.4.11) In terms of using the SMART criteria for the report's recommendations it is not clear how this particular recommendation is directly relevant to ICANN. The manner of DNS name resolution between stub and recursive name resolvers on the Internet, and the protocols used to perform such resolution appears to fall outside the scope of ICANN's activities and authority. Because of this question of direct relevance to ICANN's scope and mission, this action may be more appropriately included as part of the report's set of "suggestions," and listed on the basis of the broader topic of potential actions by ICANN org that would provide value to the community through the provision of assessments of aspects of the larger environment of the domain name space and its evolving use. The SSAC is aware of current activity within both ICANN org and the ICANN community in this space already, including a recently published SSAC study on the implications of DNS over HTTPS and DNS over TLS, and there is some lack of clarity 18 as to how this recommendation differs from current practice.	This recommendation has been removed.
ICANN Board	29.1	ICANN org should monitor and regularly report on the privacy impact of technologies like DoT (DNS over TLS) and DoH (DNS over HTTPS).	If the SSR2 RT believes additional monitoring and reporting of areas that are within ICANN org's remit are needed, the Board would encourage the SSR2 RT to provide clear statements of what issues or risks exist from the current operational model, how the SSR2 RT recommendation will address them, and what relevant metrics could be applied to assess implementation.	This recommendation has been removed.
RrSG	29.1	ICANN org should monitor and regularly report on the privacy impact of technologies like DoT (DNS over TLS) and DoH (DNS over HTTPS).	For recommendation 29.1, this appears to be outside of ICANN's remit.	This recommendation has been removed.

Source	SSR2 Section or Rec	Report Section	Comment	Response
SSAC	29.2	ICANN org's consensus policies and agreements with registry operators and registrars should, therefore, have clauses to reflect compliance with these while ensuring that the DNS is not fragmented because of the need to maintain/implement minimum requirements governing the collection, retention, escrow, transfer, and display of registration data, which includes contact information of the registrant, administrative, and technical contacts as well as technical information associated with a domain name.	(3.4.12) The introduction of the concept of DNS "fragmentation" makes no clear sense in this context. The recommendation should phrase the concern in a different way that avoids the particular term "fragmentation", or explain the concept of "fragmentation" in detail.	This recommendation has been removed.
RrSG	29.2	ICANN org's consensus policies and agreements with registry operators and registrars should, therefore, have clauses to reflect compliance with these while ensuring that the DNS is not fragmented because of the need to maintain/implement minimum requirements governing the collection, retention, escrow, transfer, and display of registration data, which includes contact information of the registrant, administrative, and technical contacts as well as technical information associated with a domain name.	The RrSG needs additional information about recommendation 29.2, as it is not clear what problem or concern this addressing- those obligations already exist.	This recommendation has been removed.
ICANN Org	29.2	SSR2 Recommendation 29.2: "with these"	Requests for clarification of terms	This recommendation has been removed.

Source	SSR2 Section or Rec	Report Section	Comment	Response
ICANN Board	29.4	ICANN org's DPO should also be responsible for external DNS PII. The DPO should provide guidance to managers and stakeholders regarding responsibilities and procedures and monitor and report on relevant technical developments.	It is unclear to the Board what it means for ICANN to "be responsible for external DNS PII."	This recommendation has been removed.
BC	30	Stay Informed on Academic Research of SSR Issues and Use That Information to Inform Policy Debates	The BC concurs with this recommendation.	Thank you. Please see Section F.2. Research and Briefings and SSR2 Recommendation 18: Informing Policy Debates for revised text.
SSAC	30	Stay Informed on Academic Research of SSR Issues and Use That Information to Inform Policy Debates	(3.4.16) In this case the recommendations appear to be specific to the point of being too prescriptive, and it would be better to propose a more general set of measures that would facilitate positive outcomes for both the ICANN community and the general academic research effort in this area of study.	Thank you. Please see Section F.2. Research and Briefings and SSR2 Recommendation 18: Informing Policy Debates for revised text.
ICANN Board	30	Stay Informed on Academic Research of SSR Issues and Use That Information to Inform Policy Debates	The Board supports the work of OCTO and its determination of the needs for data and analysis to inform its work. The Board encourages the SSR2 RT to consider if this work meets the intent of the SSR2 recommendation. If the SSR2 RT believes additional improvements are needed, the Board encourages the SSR2 RT to provide clear statements of what issues or risks exist from the current operational model, how the SSR2 recommendation will address them, and what relevant metrics could be applied to assess implementation. Further, 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.	The review team feels that the work of the entire global academic research community might be higher volume than even ICANN OCTO, but that their relevant work might best be ingested by ICANN OCTO for consideration (which is the spritit and intedended direction of this recommendation). This has been clarified in the text. Please see Section F.2. Research and Briefings and SSR2 Recommendation 18: Informing Policy Debates for revised text.
RrSG	30	Stay Informed on Academic Research of SSR Issues and Use That Information to Inform Policy Debates	It is the understanding of the RrSG that ICANN attends a lot of these events already. It is not clear from the draft report how the expense of ensuring attendence and reporting will provide signficant benefit, or where ICANN will find the funding for this initiative. Additionally, it is the position of the RrSG that these forums, which have limited (if any) participation of contracted parties, should not be the source for changes to the RAA or RA. There are already existing structures within the ICANN community for the participants of these forums to participate in ICANN's multi-stakholder model, and this proposed recommendation would circumvent that process.	The recommendation has been clarified. Please see Section F.2. Research and Briefings and SSR2 Recommendation 18: Informing Policy Debates for revised text.
RySG	30	Stay Informed on Academic Research of SSR Issues and Use That Information to Inform Policy Debates	The RySG believes that tracking academic research on DNS SSR issues should be part of ICANN's risk management strategy.	The SSR2 team welcomes the RySG's support of this recommendation. The specific implementation of this recommendation is left to ICANN org. Please see the revised text in SSR2 Recommendation 18: Informing Policy Debates.
IPC	30		The IPC is supportive of this recommendation.	Thank you. Please see Section F.2. Research and Briefings and SSR2 Recommendation 18: Informing Policy Debates for revised text.
BC	31	Clarify the SSR Implications of DNS-over-HTTP	The BC concurs with this recommendation.	This recommendation has been removed.

Source	SSR2 Section or Rec	Report Section	Comment	Response
Loganaden Velvindron	31	Clarify the SSR Implications of DNS-over-HTTP	Following the publication of: https://www.icann.org/en/system/files/files/ssr2-review-24jan20-en.pdf I note that there is a typo on page 99: DNS-over-HTTP -> DNS-over-HTTPS.	This recommendation has been removed.
SSAC	31	Clarify the SSR Implications of DNS-over-HTTP	(3.4.17) This recommendation appears to be a restatement of recommendation 29.1. ... There is merit in a more general rephrasing of this recommended action. The domain namespace is not fixed and immutable, and evolution in aspects of the use of this namespace will inevitably impact ICANN and its stakeholder community in various ways. The SSAC agrees with the general principle that ICANN and the broader community should keep themselves informed of evolutionary pressures on the domain namespace and its use. Perhaps the recommendation should be phrased in these more general terms and not specifically refer to DoH.	This recommendation has been removed.
NCSG	31	Clarify the SSR Implications of DNS-over-HTTP	#Recommendation 31: Here, we would like to ask the review team to consider the recent report produced by the SSAC, namely the SAC 109, in order to make its recommendations.	This recommendation has been removed.
RrSG	31	Clarify the SSR Implications of DNS-over-HTTP	As with many of the recommendations, this appears to be outside of ICANN's remit, the source of the funds is not clear, and the potential benefits are not defined.	This recommendation has been removed.
RySG	31		The RySG supports this recommendation.	This recommendation has been removed.
IPC	31		The IPC is supportive of this recommendation.	This recommendation has been removed.
SSAC	8, 9	Establish a Business Continuity Plan Based on ISO 22301 Ensure the Disaster Recovery Plan is Appropriate, Functional, and Well Documented	(3.2.3) The SSAC believes that the SMART methodology that the SSR2 RT adopted should be used for these recommendations. Specific and clear proposals should be phrased as to how existing BC and DR plans should be revised to meet the criteria described in relevant ISO and ISO/International Electrotechnical Commission (IEC) standards.	Recommendations 8 and 9 were merged to form SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures. The review team also noted that the detail required to make each recommendation fully SMART, including assigning appropriate timelines, will require thought and action from the implementation team and should be included in the final implementation plan.
GAC	10, 14		The GAC welcomes Recommendations 10 and 14, which aim to provide better data and enable more rigorous analysis. In this regard, the GAC highlights its commitment to evidence-based policy development and welcomes efforts to institute more systematic monitoring and evaluation of existing policy.	Thank you.
M3AAWG	11, 29	New gTLDs and the Limitations of Registrar and Registry Agreements	(6) Implement a post-GDPR Whois (and RDAP) access method that accommodates the legitimate-purpose uses of the M3AAWG membership. M3AAWG is submitting a separate comment on the EPDP Phase 2 Report. However, with regard to the SSR2 RT report, we urge the team to consistently “Ensure access to registration data for parties with legitimate purposes” which most accurately identifies the parties with need to access registration data. We further urge the review team to recommend that ICANN take no action to sunset Whois until it has determined that RDAP services are reliable, available and accurate. Lastly, we recommend that the Review Team request ICANN to conduct a study of the various (inter) relationships between registrar implementations to satisfy the EU GDPR and California’s CCPA and the privacy or proxy protection services, and to publish or establish uniform criteria for processes to obtain underlying registration data when redacted or hidden by a privacy/proxy protection service (or in some cases, both).	The SSR2 Review Team does not make a statement regarding discontinuing WHOIS. We do have further recommendations regarding privacy and access. Please see SSR2 Recommendation 16: Privacy Requirements and RDS.

Source	SSR2 Section or Rec	Report Section	Comment	Response
ICANN Board	1, 2, 5, 6, 7, 8, 9, 10.1 and 29.		The Board's draft proposal for resourcing and prioritization of community recommendations developed with input from leadership of all specific review teams, notes that an effective recommendation should address an observed issue that has significant consequences for ICANN as a whole. Clear articulation of the observed issue gives insight into the intent of the recommendation and the justification for why it should be adopted. With this in mind, the Board notes that a number of the SSR2 RT's recommendations, as currently drafted, do not clearly define the identified issues or risks, the rationale for the recommended solutions, the expected impact of implementation, or what relevant metrics could be applied to assess implementation. Some examples as outlined in this comment include SSR2 RT recommendations 1, 2, 5, 6, 7, 8, 9, 10.1 and 29.	The SSR2 Review Team took this comment into consideration during the revision of the recommendations.
ICANN Org	1, 2, 5, 6, 7, 8, 9, 15.3.4, 15.3.5, 18, 19.1, 19.2, 23.1, 26.2, and 29.2		ICANN org reiterates the Board's comment that it is helpful for the ICANN org, Board, and community to have an understanding of the particular issues or risks that each recommendation intends to address. A number of SSR2 recommendations, as currently drafted, do not clearly define the identified issues or risks, how the recommended solution will address the issues or risks, the expected impact of implementation, or what relevant metrics could be applied to assess implementation (for example, SSR2 recommendations 1, 2, 5, 6, 7, 8, 9, 15.3.4, 15.3.5, 18, 19.1, 19.2, 23.1, 26.2, and 29.2). ICANN org encourages the SSR2 RT to clarify these elements of each recommendation for the Board to properly consider the recommendations and make appropriate instructions to the ICANN org and/or community.	The SSR2 Review Team took this comment into consideration during the revision of the recommendations.
ICANN Board	1.1, 12, 15, 18.2, 19, and 29, and 22.1		The Board notes that a number of the SSR2 RT's recommendations currently directed to the Board are outside of the Board's oversight responsibilities. For example, the Board cannot unilaterally impose new obligations on contracted parties through acceptance of a recommendation from the SSR2 RT. The Registry Agreement and Registrar Accreditation Agreement (RAA) can only be modified either via a consensus policy development process or as a result of voluntary contract negotiations. In either case, the Board does not have the ability to ensure a particular outcome. The Board suggests that the SSR2 RT consider directing these recommendations either to ICANN org for inclusion in a future round of voluntary contract negotiations and/or to the GNSO Council for review as to whether the recommendation should be considered in a consensus policy development process. Some examples of recommendations to which these observations apply include SSR2 RT recommendations 11.1, 12, 15, 18.2, 19, and 29. Further, the Board suggests that the SSR2 RT consider directing SSR2 RT recommendation 22.1 to the Root Server System Governance Working Group which has recently been formed.	The SSR2 Review Team took this comment into consideration during the revision of the recommendations.
RySG	10, 11, 12, 13, 14, 15, 16		Finally, and critically, the RySG does not support the conclusions SSR2 has reached on the next steps, in particular, recommendations for unilateral contract amendments, or pre-determined outcomes of studies or policy work, as we believe both are outside the scope of SSR2's work. Reviews, while an important part of ICANN's accountability mechanisms, cannot be used to circumvent the policy development process, such as by attempting to impose new contractual obligations on contracted parties. The RySG would also ask SSR2 to refrain from making recommendations which refer to, or overlap with, existing recommendations from other reviews such as RDS-WHOIS 2, CCT-RT, Registration Data EPDP Phase 2, NCAP and potential recommendations from ATRT3.	The review team has recommended actions that we believe are within our Bylaws-mandate and scope to improve SSR and serve the public interest.

Source	SSR2 Section or Rec	Report Section	Comment	Response
i2Coalition	10, 12, 15, 16		However, the recommendations overreach this remit, in terms of ICANN's governance and functioning mechanisms, as they advocate in a number of recommendations for unilateral, top-down action from the Board or ICANN Org on new and/or under-development policy matters. Specifically, recommendation 10 (Improve the Framework to Define and Measure Registrar & Registry Compliance) which is rated with a High Importance, and has among its sub-recommendations unilaterally amending contract clauses (10.3) and closing the EPDP while unilaterally implementing a new WHOIS policy (10.4). Further, recommendation 12 outright describes the direct and sole role that the Board should play in the creation of legal and appropriate access mechanisms to WHOIS data. Even more, recommendations 15 and 16 argue for "enhancing" and "changing" contracts, respectively. All three recommendations, 12, 15 and 16 are rated High Importance. We ask that the draft report be revised to take these concerns into consideration. We believe that the topics of resilience, security, and stability are crucial, and they should be taken seriously by those in charge of reviewing them for the ICANN ecosystem. Arguing for unilateral changes to contracts and getting ahead of the Policy Development Processes are not and cannot be normal recommendations to come out of such a review.	The review team respectfully disagrees and has recommended actions that we believe are within our Bylaws-mandate and scope to improve SSR and serve the public interest. The report has been significantly revised to improve clarity.
FIRST	10,11,13		FIRST therefore welcomes the SSR2 recommendations 10, 11 and 13 and looks forward to seeing an implementation of these recommendations.	Thank you. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse, in particular SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms and SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review for updated text.
RySG	10.1, 11.2, 15.1,		the RySG encourages the SSR2-RT to spend some additional time considering what it hopes to achieve by reiterating CCT-RT recommendations, and reconsider whether they are truly necessary within an otherwise very robust set of recommendations. The RySG considers the implementation and completion of outstanding SSR1 recommendations as the key priority. In particular, the RySG believes that the remit of SSR needs to be clearly defined so that it can properly inform the scope of SSR2's work and can provide the Board with some guidance on the new recommendations.	The SSR2 Review Team has fully considered each recommendation and stands by its utlility in improving SSR.
GAC	10.3, 15.1, 15.2, 15.4, 16		The GAC invites the Review Team to consider the articulation between various Recommendations and to clarify how, for example, Recommendations 10.3, 15.1, 15.2, 15.4 and 16, which all propose changes to the contractual framework between ICANN and its Contracted Parties, should work together and be taken forward.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
GAC	10.3, 15.1, 15.2, 16		The GAC welcomes proposals for specific mechanisms as set out in Recommendations 10.3, 15.1, 15.2 and 16 to incentivize a comprehensive and effective response to DNS Abuse. The GAC has historically taken a strong interest in Registry and Registrar contractual compliance enforcement concerning WHOIS obligations, as well as other elements that affect abuse and security (See e.g., GAC Hyderabad and Copenhagen Communiqués3). Furthermore, the GAC has held regular exchanges with the ICANN Compliance Team, in writing and at its plenary meetings, in an effort to strengthen compliance mechanisms.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
RySG	11, 14, 15 and 16		We would appreciate additional information from the SSR2-RT about how it reached the decision to effectively duplicate the recommendations from a previous Review Team.	The SSR2 Review Team noted that the SSR1 recommmendations often lacked specificity, and so incorporated the intent of those original recommendations into updated recommendations with clearer guidance.

Source	SSR2 Section or Rec	Report Section	Comment	Response
RySG	11, 14, 15, 16		The RySG is also concerned with some of the definitions set out by SSR2 in Appendix A, in particular the definitions of “security threat” and “DNS abuse”, and note that we do not support the definitions provided. Given SSR2 recommends policy work by the ICANN community to define “DNS abuse” and “security threats,” the RySG would ask SSR2 to refrain from creating its own definitions. The RySG appreciates that it is useful for the SSR2 to have a working glossary to assist its work, but the working glossary should not be used to interpret the recommendations made by SSR2, or adopted as community definitions by the Board. The report seems to repeatedly conflate the terms to broadly encompass undesirable activity related to both DNS/infrastructure abuse, security threats, and IP/content-related abuse.	The lack of clear definitions that are community-accepted remains a key issue, as this comment underlines. To address this concern, SSR2 Recommendation 10.2 recommends a CCWG to create community-wide, clearly stipulated and clear definitions that can be relied upon in future.
NCSG	13, 14, 15, 16, 17, 18, 19, 20		#Recommendation 13 to 20: They are all related to DNS Abuse and the DNS operations and are “high” priorities. We recommend that the Review Team proposes a dedicated team, like a cross community Working Group to work on it. We believe that this represents a stronger way/metric to assess the effectiveness of the implementation of those recommendations by a future SSR Team rather than making specific recommendations at this point. We do not fully support the recommendations relating to the opening of DAAR data to private firms for their internal abuse department. This is outside of the role of ICANN and we do not support recommendations related to this topic. On abusive naming we reject the call to replicate the existing systems that were the result of GNSO policy making with regards to trademark confusion and string similarity, again we do not believe that this is within the mandate of the SSR2 RT.	The SSR2 Review Team has taken this feedback into consideration, and considers the items in the report to be solidly in the remit of the review team. The recommendations and associated rationale have been significantly revised.
GAC	13, 19		we also welcome Recommendations 13 and 19, which encourage the collection of data on mitigating abuse to improve Domain Abuse Activity Reporting (DAAR) in order to improve both measurement and reporting of domain abuse. Most importantly, the GAC supports the suggestion that ICANN org should publish DAAR reports identifying Registries and Registrars whose domains most contribute to abuse according to the DAAR methodology.	Thank you. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse, and in particular SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review, for updated text.
BC	13.1.1	ICANN org should publish DAAR reports that identify registries and registrars whose domains most contribute to abuse according to the DAAR methodology.	We note the 13.1.1. recommendation to publish DAAR reports in a way that “identifies registries and registrars whose domains most contribute to abuse according to the DAAR methodology”. We recommend going further than that in expanding the detail of the public DAAR reports to report activity by registry, by registrar and by measured security threat.	Thank you. Please see SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review for updated text.
RrSG	13.1.1	ICANN org should publish DAAR reports that identify registries and registrars whose domains most contribute to abuse according to the DAAR methodology.	Regarding recommendation 13.1.1, commercial entities already publish such data. Some of these reports include flawed, incomplete, or false positive information, so it is should not form the basis for ICANN to "name and shame" contracted parties. There are existing compliance activities to address registrars or registries that may not be complying with the RAA or RA. The recommendation does not mention the benefits and or possible issues such publication could create. This recommendation should be subject to community consideration before further action.	The review team notes that all recommendations are subject to public comment. Please see SSR2 Recommendation 12.3 for revised text.

Source	SSR2 Section or Rec	Report Section	Comment	Response
ICANN Org	13.1.1	ICANN org should publish DAAR reports that identify registries and registrars whose domains most contribute to abuse according to the DAAR methodology.	ICANN org is in discussions with relevant stakeholders as to how best to provide data to inform policy discussions.	The SSR2 Review Team notes that ICANN org has had several years of input and intermittent discussions without demonstrable change. Please see SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review for updated text.
RySG	13.1.1		The RySG notes that any RO can be the target of abusive activity (through no fault of the RO) and that publishing a list of victims is unlikely to curb actual abuse. We suggest instead focusing on understanding how various RO business models either (or both) prevent or mitigate abuse. DAAR data, without context, is just uncorroborated raw numbers. For instance, a particular RO may experience a 2% abuse rate as a daily average, however that number says nothing about how fast yesterday's domains were taken down and if the domains on today's list were also on yesterday's list.	The review team has taken this note into consideration. We suggest RySG provide additional information to accompany the recommended DAAR data, if they feel it's useful. Please see SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review for updated text.
RrSG	13.1.2	ICANN org should make the source data for DAAR available through the ICANN Open Data Initiative and prioritize items "daar" and "daar-summarized" of the ODI Data Asset Inventory for immediate community access.	For recommendation 13.1.2, it is not clear what source data DAAR entails, and whether the sources have been vetted by contracted parties and the broader ICANN community. The recommendation is not very clear what source data for DAAR entails. This data is likely published elsewhere, and it is not ICANN's remit to provide a clearinghouse for information that can be obtained elsewhere.	The review team considers this activity within ICANN org's remit. Please see SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review for updated text.
ICANN Org	13.1.2	SSR2 Recommendation 13.1.2: "source data"	Requests for clarification of terms	Thank you, this has been clarified. Please see SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review for updated text.
ICANN Org	13.1.2	ICANN org should make the source data for DAAR available through the ICANN Open Data Initiative and prioritize items "daar" and "daar-summarized" of the ODI Data Asset Inventory for immediate community access.	Publishable DAAR-related data is already slated to be included in the Open Data Platform.	"Publishable data" is a term ICANN org applies too narrowly and results in the publishing of DAAR data that is not actionable and falls short of what non-contracted entities have requested. Please see SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review for updated text.
RySG	13.1.2, 13.1.3		Most of the entities that collect and report on behaviors labeled "abuse" by DAAR, do so for a specific, often commercial, purpose. This data is not freely available to the world and ICANN has repeatedly explained that the contracts with the feed providers do not allow them to make the data public. We recognize that many in the community want to see this data for free and, indeed, so do many ROs. However, simply listing it as a Recommendation will not make it so.	The review team received conflicting comments and statements regarding this issue. SSR2 Recommendation 12.2 addresses this problem.

Source	SSR2 Section or Rec	Report Section	Comment	Response
RrSG	13.1.3	ICANN org should publish reports that include machine-readable formats of the data, in addition to the graphical data in current reports.	If recommendation 13.1.3 is referencing DAAR, then again, these feeds are already available.	The existing DAAR data not actionable and falls short of what non-contracted entities have requested. Please see SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review for updated text.
ICANN Org	13.1.3	ICANN org should publish reports that include machine-readable formats of the data, in addition to the graphical data in current reports.	With the inclusion of DAAR data into the Open Data Platform, this recommendation will be implemented	The review team has taken this note into consideration, and feels there is more to implementing this recommendation than just the inclusion of DAAR data into the OpenData Platform. Please see SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review for updated text.
ICANN Org	13.1.4	ICANN org should provide assistance to the Board and all constituencies, stakeholder groups and advisory committees in DAAR Interpretation, including assistance in the identification of policy and advisory activities that would enhance domain name abuse prevention and mitigation	It is unclear what sort of assistance the SSR2 RT is recommending; ICANN org asks the SSR2 RT to clarify this point. ICANN's Office of the Chief Technology Officer (OCTO) is particularly interested in ensuring people understand what DAAR data says (and doesn't say). Clarification from the SSR2 RT would be helpful.	Thank you, this has been clarified. Please see SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review for updated text.
RySG	13.1.4		ICANN org has provided a tool and information. It's the community's job to determine if that information should inspire future work.	The SSR2 Review Team agrees with this comment, and would add that ICANN org has an important role to play in informing the community about abuse so policy and other activities are based on an understanding of abuse and SSR matters.
RySG	15, 16		The RySG is concerned about a number of the recommendations that direct the Board or ICANN org to make changes to the Registry Agreement and note that it is not possible for the Board or ICANN org to unilaterally impose new contractual conditions on Contracted Parties. Amendments to the registry agreement are only possible via a formal amendment process or the adoption of consensus policies. We would therefore encourage the Review Team to reconsider the recommendations that direct the Board or ICANN org to make changes to the registry agreement as we do not believe they can be implemented.	These recommendations were misunderstood. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16 for revised text.
ICANN Org	15, 16, 19.2, 5, 6, 18, 20		ICANN org also welcomes this opportunity to provide feedback on the operational feasibility of implementation of the SSR2 RT recommendations. This comment addresses a number of recommendations that, as currently drafted, may not be feasible for ICANN org to implement because the recommendation would appear to require ICANN org to act outside of its mission and scope (for example, SSR2 recommendations 15, 16, 19.2), or the expected impact of implementation is not clearly defined (for example, SSR2 recommendations 5, 6, 18, 20). ICANN org encourages the SSR2 RT to further engage with ICANN org subject matter experts to ensure feasibility and usefulness of its recommendations.	The SSR2 Review Team took this comment into consideration during the revision of the recommendations.

Source	SSR2 Section or Rec	Report Section	Comment	Response
GAC	15, 17, 29, 31		Finally, the GAC welcomes the fact that several recommendations dovetail with priorities the GAC has endorsed for its Public Safety Working Group, such as the inclusion of ccTLDs in DNS Abuse mitigation efforts and the investigation of the security implications of DNS encryption technologies (Recommendations 15, 17, 29 and 31). The GAC invites the Review Team to consider how the work of the PSWG and other parts of the ICANN community could contribute to these efforts.	The SSR2 Review Team took this comment into consideration during the revision of the recommendations.
RrSG	15.3.1	Ensure access to registration data for parties with legitimate purposes via contractual obligations and with rigorous compliance mechanisms.	For recommendation 15.3.1, this is most likely not possible because it would violate fundamental rights of data subjects. Furthermore, the correlation between registration data and the effectiveness of actual threat mitigation is unknown.	The SSR2 Review Team disagrees with this note, and has clarified the Recommendation. Please see SSR2 Recommendation 16.2.
RrSG	15.3.2	Establish and enforce uniform Centralized Zone Data Service requirements to ensure continuous access for SSR research purposes.	Regarding recommendation 15.3.2, such research is already possible under many data protection laws. However, current ICANN community processes do not comply with these laws, and as such, the RrSG recommends that the ICANN community focus on how research in a manner that complies with existing laws (rather than making proposals that might violate those laws). The RrSG notes that ICANN OCTO has mentioned several times it does not need access to registrant data for research purposes.	The SSR2 Review Team disagrees with this note, and has clarified the Recommendation. Please see SSR2 Recommendation 11: Resolve CZDS Data Access Problems and SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review.
IPC	15.3.2		The IPC would point out that many brand owners who operate Brand TLDs under Spec 13 are reluctant to have their future branding decisions telegraphed by means of the public access to the CZDS. The Brand TLDs would encourage a more nuanced treatment of CZDS access which recognizes the particular nature of a TLD.	Thank you. The review team has taken this comment into consideration. Please see the revised text in E.2.b.ii. Centralized Zone Data Service.
IPC	15.3.3, 15.3.4		The IPC is supportive of the intent behind these recommendations but notes that ICANN has no control over ccTLDs and the ccNSO. The RT is encouraged to revisit and refine this to acknowledge this lack of control. We seek clarification as to the changes to registrant information proposed by 15.4: what changes specifically are proposed?	The recommendations indicate ccTLD involvement is voluntary. Please see clarified tesct in SSR2 Recommendation 13.1.
ICANN Org	15.3.5	Immediately instantiate a requirement for the RDAP services of contracted parties to white-list ICANN org address space and establish a process for vetting other entities that RDAP services of contracted parties will whitelist for non-rate-limited access.	ICANN org notes that this recommendation does not include justification as to why ICANN and others would need a vetting process and encourages the SSR2 RT to provide this in its final report. Further, it is not clear to ICANN org which entities the SSR2 RT intends to be vetted or how that vetting can be implemented. With regard to the request in this recommendation to "immediately instantiate a requirement", ICANN org notes that neither it nor the Board can unilaterally impose new obligations on contracted parties. The RA and RAA can only be modified either via a consensus policy development process or as a result of voluntary contract negotiations (as noted by the Board).	This has been clarified in the revised report. Please see SSR2 Recommendation 12.1.

Source	SSR2 Section or Rec	Report Section	Comment	Response
MarkMonitor	16.1.1	Contracted parties with portfolios with less than a specific percentage (e.g., 1%) of abusive domain names (as identified by commercial providers or DAAR) should receive a fee reduction (e.g., a reduction from current fees, or an increase of the current per domain name transaction fee and provide a Registrar with a discount).	MarkMonitor supports a reduction in domain fees for retaining an agreed low percentage of abusive domain names in a registrar portfolio. We believe that in the continuous fight to prevent DNS abuse and reduce “bad actors”, the positive reward for good practices should be a welcomed initiative to encourage registrars to take a proactive approach in the monitoring and enforcement actions in relation to DNS Abuse. MarkMonitor supports this novel approach to incentivise rather than chastise. In order to ensure that this is implemented successfully, we need clear definitions of the percentages to identify eligibility and also the identification method should also be defined and explained alongside the reduced fees and/ or discount.	The review team took this comment into consideration. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16 for revised text.
RrSG	16.1.1, 16.1.3	Contracted parties with portfolios with less than a specific percentage (e.g., 1%) of abusive domain names (as identified by commercial providers or DAAR) should receive a fee reduction (e.g., a reduction from current fees, or an increase of the current per domain name transaction fee and provide a Registrar with a discount). Waive RSEP fees when the RSEP filings clearly indicate how the contracted party intends to mitigate DNS abuse, and that any Registry RSEP receives pre-approval if it permits an EPP field at the Registry level to designate those domain names as under management of a verified Registrant.	For recommendation 16.1.1 and 16.1.3, how will ICANN offset the discount (which will result in a lower revenue for ICANN)?	The SSR2 Review Team is not responsible for budget allocations.
MarkMonitor	16.1.2	Registrars should receive a fee reduction for each domain name registered to a verified registrant up to an appropriate threshold.	MarkMonitor also supports this recommendation. As with 16.1.1 the success of this initiative will be with the clear and express definition of “verified”, the mechanisms that are relevant for the verification process and what the thresholds are relating to maximum submissions. This shall require more consultation with contracted parties and the review team shall need to ensure that this is implemented effectively.	The review team took this comment into consideration. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16 for revised text.

Source	SSR2 Section or Rec	Report Section	Comment	Response
RrSG	16.1.2	Registrars should receive a fee reduction for each domain name registered to a verified registrant up to an appropriate threshold.	Recommendation 16.1.2 will be difficult to implement in light of privacy laws. There are also questions, such as how can registrars verify registrants, what will prevent bad registrars from faking the verification, and does verification mean lower abuse?	The review team believes this should be addressed in the implementation plans for the recommendations in Section E. Contracts, Compliance, and Transparency around DNS Abuse.
ICANN Org	16.1.2	SSR2 Recommendation 16.1.2: “verified registrant”	Requests for clarification of terms	The review team believes this should be addressed in the implementation plans for the recommendations in Section E. Contracts, Compliance, and Transparency around DNS Abuse.
ICANN Org	16.1.2	Registrars should receive a fee reduction for each domain name registered to a verified registrant up to an appropriate threshold.	As noted in the section “Requests for Clarification of Terms,” ICANN org seeks clarification of the term “verified registrant”. Is the SSR2 RT referring to potential activities to “verify” the identity of a registrant? If this is the case, ICANN org encourages the SSR2 RT to consider this recommendation in light of ongoing discussions and work related to the European General Data Protection Regulation (GDPR), including the feasibility of conducting such activities in light of GDPR, and the impact on ICANN contracts. Specifically, depending on what the SSR2 RT means by “verified registrant”, conducting verification activities could have potential implications for ongoing discussions related to access to non-public registration data as well as controllership. That is, who does the SSR2 RT envision would be conducting the verification and managing the data related to verified registrants? Additionally, ICANN org encourages the SSR2 RT to consider the potential budgetary implications of a fee reduction.	The review team believes this should be addressed in the implementation plans for the recommendations in Section E. Contracts, Compliance, and Transparency around DNS Abuse.
MarkMonitor	16.1.3	Waive RSEP fees when the RSEP filings clearly indicate how the contracted party intends to mitigate DNS abuse, and that any Registry RSEP receives pre-approval if it permits an EPP field at the Registry level to designate those domain names as under management of a verified Registrant.	MarkMonitor supports this offering and appreciates the approach of ensuring that there is an incentive for the registry in addition to registrars.	Thank you. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16 for revised text.
ICANN Org	16.1.3	Waive RSEP fees when the RSEP filings clearly indicate how the contracted party intends to mitigate DNS abuse, and that any Registry RSEP receives pre-approval if it permits an EPP field at the Registry level to designate those domain names as under management of a verified Registrant.	ICANN org notes that there are no fees for submitting Registry Services Evaluation Policy requests (RSEPs). Fees only apply if ICANN org identifies potential security or stability concerns and utilizes a Registry Services Technical Evaluation Panel (RSTEP). Is the SSR2 RT referring to RSTEP fees in this recommendation? Further, ICANN org notes concerns regarding the feasibility of implementing this recommendation as pre-approval may not be possible. ICANN org encourages the SSR2 RT to consider in its final recommendation if the Fast Track RSEP Process could be utilized to meet the intended outcome of this recommendation.	The review team took this comment into consideration. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16 for revised text.

Source	SSR2 Section or Rec	Report Section	Comment	Response
MarkMonitor	16.1.4	Refund fees collected from registrars and registries on domains that are identified as abuse and security threats and are taken down within an appropriate period after registration (e.g., 30 days after the domain is registered).	MarkMonitor supports this recommendation, however we are aware that the implementation of this scheme may require considerable effort from a policy perspective. As this specific recommendation shall require clear parameters, especially the provision of what is an “appropriate” period. As per our comments and feedback, specificity is vital in the successful implementation of these initiatives and this scheme is exactly in the same vein. Also clarifying the mechanisms of how we shall identify the domain names, what constitutes a valid “take down” and what is “appropriate” will severely minimise the scope for this DNS Abuse initiative being abused itself. This shall require the most consultation from contracting parties. Ultimately MarkMonitor supports rewarding actions by contracted parties to address new forms of abuse.	The review team took this comment into consideration. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16 for revised text.
RrSG	16.1.4	Refund fees collected from registrars and registries on domains that are identified as abuse and security threats and are taken down within an appropriate period after registration (e.g., 30 days after the domain is registered).	It is not clear how recommendation 16.1.4 can be tracked. As with other parts of this recommendation, it is subject to gaming/abuse. It could also lead to a new version of frontrunning (e.g. register a domain, track traffic for 25 days, then suspend for "abuse" to get money back if the domain is not generating sufficient parking page revenue or a malicious campaign ends).	The review team took this comment into consideration. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16 for revised text.
ICANN Org	16.1.4	Refund fees collected from registrars and registries on domains that are identified as abuse and security threats and are taken down within an appropriate period after registration (e.g., 30 days after the domain is registered).	ICANN org repeats its comments above with regard to SSR2 Recommendation 15.1, namely that consideration should be given to the ongoing community discussions regarding the definition of “DNS abuse” as well as metrics/reporting for abuse. Additionally, ICANN org has concerns with regard to how this recommendation could be effectively implemented and encourages the SSR2 RT to consider potential issues with gaming and mis-aligned incentives. For example, contracted parties might have less incentive to guard against the creation of domains intended for misuse or might in some cases even profit from their creation if they end up being “free” of ICANN transaction fees.	The review team took this comment into consideration. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16 for revised text.
IPC	16.1.4		The IPC does not understand what is intended by this recommendation. It would appear to create the possibility of a bad-actor registrar selling such names and then rapidly taking them down, thereby receiving payment both from the registrant and a refund from ICANN. This presumably is not the intent, so the RT may wish to clarify this recommendation.	The review team took this comment into consideration. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16 for revised text.

Source	SSR2 Section or Rec	Report Section	Comment	Response
ICANN Org	2, 3.4, 4.1, 5, 7, 8, 9, 22.4, 25.2,13 and 21		Work is already underway by ICANN org, community, and/or Board to address issues identified by SSR2 RT and the subject of some of these recommendations. It is not clear if the SSR2 RT considered the briefings, background material, or responses to information requests about work underway when formulating its recommendations. ICANN org encourages the SSR2 RT to consider this work to determine if it addresses the identified issue/risk. If the SSR2 RT's intent is to recommend implementation of something beyond what has already been implemented, ICANN org encourages the SSR2 RT to clarify what issues or risks exist from the current operational model, how the SSR2 RT recommendations will address them, and what relevant metrics could be applied to assess implementation. Some examples of recommendations that ICANN org considers to already be implemented include SSR2 Recommendations 2, 3.4, 4.1, 5, 7, 8, 9, 22.4, 25.2. Work is already underway to address issues identified by SSR2 Recommendations 13 and 21.	The SSR2 Review Team considered ongoing work up to January 2020. In order to finish the report, the review team needed to stop tracking and considering additional information about ongoing activities.
ICANN Board	2,5,7,8,9		In connection with these recommendations addressing various aspects of risk management within ICANN org, the Board requests clarification as to what issues or risks exist from the current operational model, how the SSR2 RT recommendations will address them, and what relevant metrics could be applied to assess implementation. ... The Board considers the policies, plans, and programs that ICANN org has in place to be appropriate and therefore considers these recommendations already to be operational and part of the Board's regular oversight responsibility. If the SSR2 RT does not agree with the Board's assessment, the Board requests the recommendation explain what is missing, the risks associated, how SSR2 RT suggests those risks should be addressed, and what relevant metrics could be applied to assess implementation.	The review team took this comment into consideration. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16 for revised text.
SSAC	24, 25		(3.3.25) The section relating to root zone Data and Internet Assigned Numbers Authority (IANA) Registries seems to contain a mix of considerations relating to the content of 15 the root zone of the DNS, the work of maintaining a collection of protocol parameter registries as a service to the IETF, and the Centralized Zone Data Service (CZDS), which appears to be a service that is a component of the ICANN gTLD DNS function. It may be helpful for the report to independently consider these areas.	The review team took this comment into consideration. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 11: Resolve CZDS Data Access Problems, and SSR2 Recommendation 22: Service Measurements for revised text.
RrSG	29.3.1	Create specialized units within the contract compliance function that focus on 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 evolving RDAP framework.	For recommendation 29.3.1, it is the position of the RrSG that Compliance should be allowed to determine its structure and functions without community interference. If this recommendation is adopted, then Compliance would be subject to control by other areas of the ICANN community (and other structures within ICANN as well).	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.

Source	SSR2 Section or Rec	Report Section	Comment	Response
SSAC	29.3.2	Monitor relevant and evolving privacy legislation (e.g., CCPA and legislation protecting personally identifiable information (PII)) and ensure that ICANN org's policies and procedures are aligned and in compliance with privacy requirements and the protection of personally identifiable information as required by relevant legislation and regulation	(3.4.13) This recommendation appears to present certain logistical challenges for ICANN org to ensure that ICANN policies and procedures are aligned and in compliance with privacy requirements across all legislative regimes, as the recommendation proposes. Within the review's adopted approach of phrasing SMART recommendations it is unclear how these logistical challenges are to be measured and tracked. The reference to "relevant legislation and regulation" might benefit from a more specific formulation that takes into account the considerable spectrum of variance of national regulations in this space.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
ICANN Board	29.3.2	Monitor relevant and evolving privacy legislation (e.g., CCPA and legislation protecting personally identifiable information (PII)) and ensure that ICANN org's policies and procedures are aligned and in compliance with privacy requirements and the protection of personally identifiable information as required by relevant legislation and regulation	The Board notes that ICANN org regularly publishes reports on global legislative and regulatory developments (including privacy legislation) to identify legislative efforts across the globe early-on, to raise awareness within ICANN, and allow for potential impacts to be considered. Additionally, the Board recently took action on the RDS-WHOIS2 Final Report and recommendations, including two recommendations that call for monitoring of legislative and policy development around the world - R1.1 and R1.2. The Board approved these recommendations, noting that corresponding activities are already part of ICANN's plans. The Board encourages the SSR2 RT to consider if this work meets the intent of the SSR2 recommendation. If the SSR2 RT believes additional improvements are needed, the Board encourages the SSR2 RT to provide clear statements on what issues or risks exist from the current operational model, how the SSR2 recommendation will address them, and what relevant metrics could be applied to assess implementation.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
RrSG	29.3.2	Monitor relevant and evolving privacy legislation (e.g., CCPA and legislation protecting personally identifiable information (PII)) and ensure that ICANN org's policies and procedures are aligned and in compliance with privacy requirements and the protection of personally identifiable information as required by relevant legislation and regulation.	Regarding recommendation 29.3.2, it is the understanding of the RrSG that ICANN already does this, with a focus on all laws that could impact the ICANN community.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.

Source	SSR2 Section or Rec	Report Section	Comment	Response
SSAC	29.3.3	Develop and keep up to date a policy for the protection of personally identifiable information. The policy should be communicated to all persons involved in the processing of personally identifiable information. Technical and organizational measures to appropriately protect PII should be implemented.	(3.4.14) The SSAC agrees with the principle behind this recommendation. However, the recommendation appears to imply that ICANN does not have such a policy already, as the recommendation calls for the development of such a policy. To what extent does the ICANN Privacy Policy fall short of the objectives of this recommendation?	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
ICANN Board	29.3.3	Develop and keep up to date a policy for the protection of personally identifiable information. The policy should be communicated to all persons involved in the processing of personally identifiable information. Technical and organizational measures to appropriately protect PII should be implemented.	The intent of the draft recommendation is unclear to the Board.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
RrSG	29.3.3	Develop and keep up to date a policy for the protection of personally identifiable information. The policy should be communicated to all persons involved in the processing of personally identifiable information. Technical and organizational measures to appropriately protect PII should be implemented.	For recommendation 29.3.3, ICANN org should already do this, and this is already covered in the RAA and RA.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.

Source	SSR2 Section or Rec	Report Section	Comment	Response
SSAC	29.3.4	Conduct periodic audits of adherence to privacy policies implemented by registrars to ensure that they, at a minimum, have procedures in place to address privacy breaches.	(3.4.15) This recommendation lacks clarity and appears to lack measurable outcomes.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
ICANN Board	29.3.4	Conduct periodic audits of adherence to privacy policies implemented by registrars to ensure that they, at a minimum, have procedures in place to address privacy breaches.	ICANN Contractual Compliance cannot audit something that is not an ICANN contractual requirement. ... The RA and RAA can only be modified either via a policy development process (PDP) or as a result of contract negotiations. In either case, the Board does not have the ability to ensure a particular outcome."	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
RrSG	29.3.4	Conduct periodic audits of adherence to privacy policies implemented by registrars to ensure that they, at a minimum, have procedures in place to address privacy breaches.	For recommendation 29.3.4, ICANN Compliance already has an audit program. The RrSG need more information regarding recommendation 29.4 as it is not clear what "external DNS PII" refers to.	The SSR2 Review Team's recommendations regarding compliance have been significantly revised. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16.
FIRST	7, 11, 14, 17		Much of the SSR activities support these goals, yet the recommendations seem to focus mostly on technical and procedural aspects and neglect the soft fabric of the global Internet community. In particular FIRST suggests, that the following points are taken into consideration ● ICANN prompt that all registries operate incident response teams ● ICNAN promotes and enforces responsible behaviour for registrars ● ICANN works toward a standard to report abuse to registries and registrars ● ICANN develops in a true multistakeholder fashion the development of norms for the domain industry to fight cybercrime.	The review team took this comment into consideration. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16 for revised text.
ALAC	Abuse and Compliance		The ALAC has a particular focus on and interest in DNS Abuse. To address this may require contractual changes to facilitate Contractual Compliance action. Such changes require either negotiations with the contracted parties or a PDP. A PDP will take considerable time and the ALAC does not advocate such a path, but rather it is time for ICANN Org and specifically Contractual Compliance to meet with those contracted parties who have shown an interest in DNS Abuse mitigation, and come to an agreement on needed contractual changes, factoring in not only penalties but any incentives that can be reasonably provided to encourage compliance.	The review team took this comment into consideration. Please see Section E. Contracts, Compliance, and Transparency around DNS Abuse and SSR2 Recommendation 8 through 16 for revised text.

Source	SSR2 Section or Rec	Report Section	Comment	Response
SSAC	Appendix D	Findings Related to SSR1 Recommendations	(3.1.11) Appendix D enumerates each SSR1 Recommendation and assesses the level of implementation. This section of the report starts by summarizing the SSR2 RT's understanding of the reasons for the incomplete implementation of the SSR1 Recommendations: ... The SSAC believes that these observations merit further consideration. The SSAC suggests that one way for the report to prompt such consideration is to rephrase these observations as proposals for implementation in the form of Recommendations in the main body of the document.	The review team took this comment into consideration and consolidated the SSR1 gaps into the SSR2 recommendations.
SSAC	Further Suggestions		(3.5.1) The report contains an appendix titled "Further Suggestions" with 5 suggestions listed in this section. This section has some of the characteristics of a record of responses to 21 some of the challenges of the SSR2 RT in undertaking this review, but without any motivating text it is challenging to understand the purpose of this section of the report. It would be helpful if the report could clarify the RT's intentions in listing these suggestions. What is the status of these suggestions? Are they formal recommendations? If not, then what is the intended status of the work items that are listed here?	As noted in the Executive Summary, "To support more efficient evaluations by future SSR review teams, the SSR2 Review Team attempted to phrase its own recommendations according to the SMART criteria: specific, measurable, assignable, relevant, and trackable. In many cases, the detail required to make each recommendation fully SMART, including assigning appropriate timelines, will require thought and action from the implementation team and should be included in the final implementation plan."
SSAC	Summary	All	(2.1) The SSR2 RT should consider adding such an environmental assessment, inventory, and a strengths and weaknesses assessment to the final report, as this would be helpful to many readers, and make the report more actionable and easier to prioritize.	A full environmental assessment is impossible to do well with existing volunteer resources. Furthermore, the SSR2 Review Team did not have access to relevant / necessary materials to conduct such an analysis in a useful manner.
SSAC	Summary	All	(2.1) Further prioritization and consolidation of issues should be considered to make the report stronger.	The report has been significantly revised, and the review team reassessed all assigned priorities.
SSAC	Summary	All	(2.3) It would be helpful if the SSR2 RT provided context and reasoning to substantiate each of the recommendations within the body of the report. It would also be helpful if they described the intention of the recommendations in terms of the resulting benefit and cost to the ICANN org, and ICANN community, if these particular recommendations were to be implemented.	The SSR2 Review Team has tried to identifiy benefits for implementing each recommendation and the harm that will come if the recommendation is not implemented. Further work regarding costs should be determined in the implementation planning stage.
SSAC	Summary		(3) The Summary of SSR2 recommendations notes that, "the SSR2 RT removed any recommendations from this report that did not clearly align with the strategic plan." ... The SSAC is concerned about the possibility of relevant and useful considerations that impact security and stability have been removed from this report. Even if they are not recommendations, such material should be noted in this report.	The review team aligned closely with the strategic plan in order to avoid stepping beyond ICANN's remit. Please see Appendix G: Mapping of SSR2 Recommendations to the ICANN 2021-2025 Strategic Plan and the ICANN Bylaws.
SSAC	Summary		(3) The SSAC believes it would be helpful for the report to indicate how these priorities were calculated.	Please see Section B.2. Prioritization.
SSAC	Summary		(3) the SSR2 RT might consider rearranging their final report along this [an overarching structured matrix as found in ISO 27001/2 or NIST CSF compliance frameworks] structure, time permitting.	Thank you, but this would have required more resources than the review team had available. Note that the report has been significantly revised to minimize duplication and improve clarity.
NCSG	Summary		we require the SSR2 team to define what the priority levels actually mean. For instance, within what timeframe/deadlines should a priority "high" recommendation be started, implemented, and reviewed?	The review team did not work against any definitions beyond an ordinal scale open to the input of the individual review team members. Please see Section B.2. Prioritization.
ALAC	Summary		The ALAC also notes that in the opinion of the SSR2 RT, many of the recommendations are deemed to be of high priority. Given the current interest in ICANN of prioritizing activities with the implicit effect of not addressing those lower on the list, this could lead to not addressing issues critical to the SSR of the DNS. ... Given the potential for rejection or deferral of the large number of high priority items, the ALAC encourages the review team to strengthen the justification on the high priority items.	The report has been significantly revised, and the review team reassessed all assigned priorities.

Source	SSR2 Section or Rec	Report Section	Comment	Response
ICANN Board	Summary		The Board reminds the SSR2 RT that the degree of consensus or agreement reached by the SSR2 RT on each recommendation should be clearly noted in the SSR2 RT's final report, in accordance with the ICANN Bylaws Section 4.6.	The final report will include this information.
RySG	Summary		We strongly urge SSR2 to reconsider its prioritization of recommendations and bundle recommendations where they are similar or form a part of a "package," and then stack rank the bundles for priorities.	The report has been significantly revised, and the review team reassessed all assigned priorities.
GAC	Summary		The GAC welcomes the endorsement of many of the Competition, Consumer Trust and Consumer Choice Review (CCT Review) and Registration Directory Service Review (RDS-WHOIS2 Review) findings and Recommendations. The independent endorsement by three separate cross-community review teams of the same recommendations should be viewed as a strong incentive for swift action. At the same time, the need to repeat identical recommendations or endorsements thereof, shows a mounting concern regarding the state of their implementation.	The report has been significantly revised, and the review team reassessed all assigned priorities.
IPC	Summary		In closing, the IPC notes that the RT has made 31 recommendations, most of which have multiple sub-recommendations, and most of these are assigned a 'high priority' by the RT. We would simply caution that spirit and intent of the Operating Standards for Specific Reviews1 encourage RTs to categorize each recommendation as 'high priority', 'medium priority', or 'low priority', as a useful guideline for the planning of the implementation work. This prioritization is intended to assist Org and the community and to try to minimize volunteer exhaustion. The RT could greatly assist the community by being more selective in prioritization for their Final Report.	The report has been significantly revised, and the review team reassessed all assigned priorities.
IPC	Summary		The IPC also notes that the recent Operating Standards for Specific Reviews also ask that recommendations "provide specific, measurable, achievable, realistic, and time-bound (SMART) recommendations based on fact-based findings. The review team is strongly encouraged to lay out problems it discovered and explain how its recommendations will address these, leading to substantive improvements. To facilitate the eventual implementation of its recommendations, the review team shall include, wherever possible, relevant metrics and applicable key performance indicators (KPIs) that could be applied to assess the implementation of each of its recommendations." The IPC commends the RT for having produced a report which is well-structured and easy to navigate and read. Based on the IPC's experience with other Reviews, and particularly on the time that it can take to track back through the recommendations of earlier iterations of a specific review, the IPC asks the RT to consider whether it would be feasible for its recommendations to also be presented in a manner where the recommendation, the problem it addresses and how it does so, together with any KPIs, are clearly laid out together in a tabular form, perhaps in an annex. The IPC believes that this would assist both the next SSR RT when they come to assess the implementation and effectiveness of the SSR2 recommendations, and the community during the subsequent public comment process.	The operating standards for specific reviews was adopted after the SSR2 Review Team started their work; the group did not change course to comply with those standards. The review team indicates in Section A. Executive Summary that "the detail required to make each recommendation fully SMART, including assigning appropriate timelines, will require thought and action from the implementation team and should be included in the final implementation plan."
SSAC	Workstream 2		(2.2) Some SSAC reviewers believe that it would be helpful for the community and helpful in terms of overall accountability for SSR2 to have included an assessment of the extent to which the ICANN community, ICANN Board, and ICANN org are operating effectively from a security and stability perspective.	The SSR2 Review Team has suggested actions that we beliveve will improve SSR, but we do not intend to produce a "report card" for the community, Board, or org. ICANN org may consider creating such a report card as part of its overall implementation of these recommendations.

Source	SSR2 Section or Rec	Report Section	Comment	Response
NCSG	Workstream 3		Globally, we have noted that the recommendations made here are pertinent, nevertheless, their measurability would pose a problem. Although the SSR2 Team recommends ICANN to define some metrics for the different evaluation and assessment, the review team was not very specific, leaving open how and what metrics will be set. We are afraid this will lead to the same situation as after SSR1, when most of the recommendations were only partially implemented and were difficult to assess. Also, as a reminder, there is still a citation (page 31 of the report) left to be added, for accuracy. We also caution against the report being used to expand ICANN's remit beyond its current mandate. While DNS abuse is a critical topic, much of the responsibility for structural addressing of this threat rests outside of ICANN's remit.	