SSR2 Review Team Recommendations

In light of the information gathers and analysis carried out for this review, the SSR2 Review Team has developed recommendations that fall into several categories:

- Making review easier for future review teams;
- Complete the implementation of SSR1 Recommendations;
-

The review team's recommendations are summarized in the table below. The full recommendations follow the table. The review team agreed on the priority assigned to each of the recommendations:

- **High priority**: To be implemented within 18 months of the issuance of a final report.
- **Medium priority**: To be implemented with 36 months of the issuance of a final report.
- **Low priority**: To be implemented prior to the start of the next SSR Review.

Making review easier for future review teams

Finding information about public comments can me quite challenging. This recommendation will allow future review teams to more easily find information using readily available mail archive search tools.

Recommendation 1 (High Priority)

To facilitate the investigation after public comment is over, ICANN should create an email list for announcements about public comment. At least three messages should be sent to this email list for each public comment activity. The first message should be sent at the opening of public comment, and it should include a stable URL to the draft document. The second message should be sent at the closing of public comment, and it should include a stable URL to the collection of submitted comments. The third message should indicate whether consensus was reached, and if so, it should include a stable URL to the final document. Other messages might also be useful, such as an extension to the comment period. In addition, ICANN shall consider having a web page dedicated to listing all public calls for comments which would then be linked to the page of the relevant document.

Complete the implementation of SSR1 Recommendations

SSR1 Recommendation 6: The roles and responsibilities for SSAC and RSSAC are captured in a public document, but it is still marked as "DRAFT UNDER REVIEW." If consensus was achieved, a final document could not be located. The SSR1 recommendation calls for a consensus

document. It appears that work was started on this recommendation; however, it concluded without addressing organizational reviews of SSAC and RSSAC.

Recommendation 2 (Medium Priority)

ICANN should fully implement the SSR1 Recommendation 6. ICANN should update the draft document from March 2015 that describes SSAC and RSSAC responsibilities to resolve the comments from SSAC and RSSAC, and then the public comment should be resumed or repeated. Once consensus is reached, ICANN should produce a final document with a stable URL.

SSR1 Recommendation 9: While ICANN runs specific infrastructure that some standards might struggle to capture appropriately, there is value in pursuing individual and organisational certifications, particularly where these goals are organised and planned appropriately. ICANN should be audited and certified along the lines of various standards, and should assess certification options with commonly accepted international standards (e.g. ITIL, ISO, SSAE-16) for its operational responsibilities.

Recommendation 3 (High Priority)

ICANN should fully implement the SSR1 Recommendation 9. Establish a road map of the certification activities that are being undertaken, including goal dates for obtaining each certification. ICANN should also provide reasoning for their choices, demonstrating how the certifications fit into ICANN's security and risk management strategies. In order to reap the benefits of a certification and audit regimen, ICANN Org should set and communicate expectations for organisational and individual audits and certifications, and explain how their expectations and plans are appropriate. ICANN Org should explain which certifications or trainings are relevant to which roles in the organisation, and track completion rates.

SSR1 Recommendation 11: While actions have been taken to mitigate domain name abuse, the implementation did not have its intended effect. SSR1 Recommendation 11 was aimed at embedding SSR considerations into the expansion of the DNS space (either through the new gTLD program or the ccTLD IDN Fast Track) through appropriate metrics and risk mitigation measures. Measures for success that have community consensus are needed.

Recommendation 4 (High Priority)

ICANN should fully implement the SSR1 Recommendation 11. ICANN should implement coordinated vulnerability disclosure reporting, including a clear communication plan for reports to the entire community.

SSR1 Recommendation 12: Cybersecurity threats are becoming more acute, and several countries are adopting specific cybersecurity strategies. Maintaining and improving the SSR of the domain name system is a limited but essential part of ensuring the SSR of the Internet. Further work is needed to fulfil the objectives of SSR1 Recommendation 12 and create a proactive environment for the community to improve SSR throughout the Internet.

Recommendation 5 (Medium Priority)

ICANN should fully implement the SSR1 Recommendation 12. ICANN should work with the community to capture SSR-related best practices in a consensus document, and then implement the practices in contracts, agreements, and MOUs.

SSR1 Recommendation 15: ICANN has implemented a vulnerability disclosure process; however, there are no public statistics or other information on how often such a process has been invoked. While a process exists, it is not possible to assess if that process is functional and effective.

Recommendation 6 (Medium Priority)

ICANN should fully implement the SSR1 Recommendation 15. ICANN should produce regular and timely reporting of anonymous metrics on the vulnerability disclosure process.

SSR1 Recommendation 16: While the recommendation was partly implemented, it s it is not clear how information is systematically incorporated. In particular, this recommendation envisions greater public engagement with SSR initiatives, including the Frameworks and Annual Reports. However, the implementation resulted in no obvious changes to the way the SSR Framework and Annual Reports are created. It is not clear how process changes related to SSR activities have expanded participation and input.

Recommendation 7 (Medium Priority)

ICANN should fully implement the SSR1 Recommendation 16. ICANN should develop an overarching SSR strategy that includes measurable and trackable objectives pertaining to the acquisition of external feedback and outreach to relevant stakeholders, both inside and outside the community.

SSR1 Recommendation 18: While there might be an informal or undocumented internal process, the implementation did not provide a public, annual, operational review of the implementation of the SSR Framework.

Recommendation 8 (Medium Priority)

ICANN should fully implement the SSR1 Recommendation 18. ICANN should update the SSR Framework each year. An operational review of progress toward implementing the SSR Framework should be a component of the following year's SSR Framework.

SSR1 Recommendation 20: SSR-related activities appear in ICANN's annual budget, but only at a very high level. This recommendation intended a greater degree of granularity for examination and public comment of SSR-related budget items.

Recommendation 9 (High Priority)

ICANN should fully implement the SSR1 Recommendation 20. ICANN should be fully transparent with the budget for parts of the ICANN Org related to implementing the SSR Framework and performing SSR-related functions.

SSR1 Recommendation 22: For the purposes of transparency and accountability, documentation for the SSR-related budget, resources, and activities related to the new gTLD program.

Recommendation 10 (Medium Priority)

ICANN should fully implement the SSR1 Recommendation 22. ICANN should publish, monitor, and update documentation on the organization and budget resources needed to manage SSR-related issues associated with the introduction of new gTLDs.

SSR1 Recommendation 27: Publicly available information as to how risk management is addressed can be found in piecemeal locations. It is clear that there are staff members representing each function involved in implementing the risk framework; however, the risk function for ICANN Org is not centralised and strategically coordinated.

Recommendation 11 (Medium Priority)

ICANN should fully implement the SSR1 Recommendation 27. ICANN's Risk Management Framework should be clearly articulated, aligned strategically against the requirements and objectives of the Organization, describe relevant measures of success, and how these are to be assessed.

In addition, the SSR2 Review Team notes the conclusion of the DNS Risk Framework Working Group, its report, and the 2016 Identifier Systems Security, Stability and Resiliency Framework for FY 15-16. These should to be taken into account for the development of RIsk Management Frameworks.

SSR1 Recommendation 28: While the SSR2 Review Team is confident that ICANN plays a coordinating role in distributing threat intelligence to involved parties and engages regularly with law enforcement, there is little or no public evidence. Furthermore, there is no public evidence that the ICANN Org conducts ongoing threat detection. The ICANN community, however, has a number of groups (both open and closed) that actively conduct threat detection.

Recommendation 11 (Medium Priority)

ICANN should fully implement the SSR1 Recommendation 28. ICANN should actively engage in threat detection and mitigation, actively participate in efforts to distribute threat and incident information, and provide public evidence that these activities have occurred.

Comments / Ideas:

Should ICANN support the development / improvements relating to SSR issues within the DNS protocols?