Preamble for SSR1 Recommendations

In 2012, the ICANN Board found *"that the 28 Recommendations in the [SSR1] Final Report are feasible and implementable,"* and unanimously accepted and instructed staff to implement all 28 SSR1 recommendations. One of the SSR2 tasks was assessing "*the extent to which prior SSR Review recommendations have been implemented and the extent to which implementation of such recommendations has resulted in the intended effect.*"

The SSR2 review team performed this assessment from its inception until the end of 2018 (exclusive of the period of suspension by the ICANN Board of the team's work that occurred Oct. 2017 — June 2018). This preamble contextualizes the team's process and methodology. The "process and method" section outlines the assessment process, the types of evidence and data used, and finally the methodology adopted in reaching a conclusion on the level of implementation of the recommendations. Each review is a learning opportunity and the "takeaways" section describes our lessons learned. Most importantly, having undertaken the assessment of the SSR1 Recommendations, the SSR2 notes the importance and the necessity to provide recommendations that are metric-based with measurable performance indicators. This observation is underpinned by the need to ensure effective implementation and assessment of any of ICANN's review team's recommendations..

Process and method:

The assessment process of the SSR2 review team outlined below is based on: briefings from, and discussions with, ICANN Org staff responsible for implementation; the systematic review of a substantial amount of relevant ICANN documents and implementation reports created by ICANN Org; and additional research and Interviews. The team also used outreach sessions in Barcelona and Kobe to liaise with relevant community stakeholders. The assessment was both quantitative and qualitative, wherever possible, depending on the specific recommendation.

Many SSR1 recommendations were high level and lacked specificity. The SSR2 team also had no authority to access and analyze the internal workings of ICANN, and thus asked ICANN Org to provide their implementation plans and evidence of successful implementation to the review team members. The recommendations themselves, and the documentation provided by ICANN Org lacked defined KPIs and targets,

measurable objectives, and implementation plans. This made the measurement or tracking of the implementations challenging. Furthermore, the wording of some of the recommendations left room for interpretation. This occasionally led to a different understanding of the recommendation by the SSR2 team from the one used by ICANN Org staff.

For each recommendation, ICANN Org staff provided initial answers on implementation to the team in 2017, reporting on how they implemented the SSR1 recommendations, and providing evidence and documentation to satisfy to the team that implementation had been completed successfully. ICANN staff cited web pages or documents, arranged presentations from various departments within ICANN Org and also provided the team with briefings on the recommendations over nine months. The team also reviewed a substantial number of background documents relevant to this review. For each recommendation, the report provides a list of all documents used by the SSR2 team and answered questions by ICANN Org staff.

In order to allocate its time and resources efficiently, the team first performed research and investigation based on these available or provided materials in 2017. Then, the team focused its further efforts on specific SSR issues and open questions identified by this initial review. The team conducted interviews with ICANN Org staff, requested additional information, and used the input of relevant stakeholders and its own research to conduct further analysis where appropriate.

After receiving replies to the questions submitted, and completing its research and due diligence to the best of its ability, the team drafted strawman assessments for each recommendation in mid to late 2018, which were discussed online, on the team's weekly calls, and in face-to-face meetings. The team edited text as needed, and approved the conclusions and findings for each SSR1 recommendation with the intention for its inclusion in the draft SSR2 team report, with the team's approved consensus protocols, and noting minority objections where applicable.

After discussing online and on calls, and going through multiple iterations, the team decided to structure their assessment draft according to the following methodology, which focused on task completion, relevance, and further work required:

1. What was done to implement the recommendation?
2. Was the recommendation fully implemented?
3. Did the implementation have the intended effect?

4. How was the assessment conducted?
5. Is the recommendation still relevant today?
6. If so, what further work needed? If not, why not?[1]

The first question speaks to what ICANN Org did to implement the recommendation. Question two gives the team's assessment of the level of implementation as of the "fully implemented date" provided by staff. The team encountered many recommendations that seem to have been only partially implemented or where implementation plans were missing. In these cases, the team identified specific areas for improvement. In some cases, it was difficult to establish clear preconditions and targets necessary for successful implementation due to missing implementation plans, documentation, and missing performance indicators. The third question addresses if and to what extent the implementation had the intended effect. The fourth question speaks to how the SSR2 team conducted the assessment. Readers can trace documents and other evidence used by the team on a per-recommendation basis. Based on question five, the team also evaluated whether each recommendation was still relevant in 2018. Finally, the team then decided whether current circumstances warrant additional work to implement a form of this recommendation, which would then inform the SSR2 team's own set of recommendations.

Takeaways:

In order to allow easier implementation going forward, the review team will strive to phrase its own recommendations according to the *SMART* criteria. This means that wherever possible, recommendations will be *specific, measurable, assignable, relevant, and trackable*. It is the review team's belief that clearer and action-oriented recommendations will simplify implementation, tracking, and the assessment process to be undertaken by the next SSR review.

[1] This structure was first outlined by Russ Housley on the 10th of September 2018 and agreed on by the team after trying it out on several of the SSR1 recommendations.

Summary

The SSR2 Review Team reviewed all 28 SSR1 recommendations, and found that out of 28 recommendations, 27 remain relevant at this point in time. The team considers no recommendation to be implemented in full, for the reasons outlined in the next section. Instead, the team found partial implementations of 26 SSR1 recommendations, and found 2 to be not implemented. Further information is provided in table 1.

Table 1: Recommendation Overview

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Relevant	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
Implemented	P	P	P	P	P	N	P	P	N	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Work needed	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y

While the detailed assessment below speaks to the specific implementations, their issues, and the team's ideas for further work, the team notes the following reappearing issues:

1. There is a lack of indicators, measurement, and goalposts that would allow the community and ICANN Org to track and understand the security space and their own activities.

2. There is a lack of publicly available evidence, definitions, and procedures, inhibiting observation of SSR activities. This leads to a lack of clarity regarding what is being done, when it is done, by whom, and how.

3. There is also a lack of community review and accountability, denying the ICANN community opportunities to provide input on SSR matters.

4. ICANN does not currently have an overarching strategy, identifiable goals, or a clear and comprehensive SSR policy. Without integrated security and risk

management (e.g. policy, procedures, standards, baselines, guidelines), it is difficult to build a functional SSR strategy, and it leads to a lack of accountability, as SSR responsibilities are not assigned and tracked.

The SSR2 review finds that ICANN's implementation of the SSR1 recommendations is incomplete. The team notes that the open, untrackable nature of the SSR1 recommendations contributes to partial implementations, as noted in the preamble. However, the team also finds a lack of accountability and transparency when it comes to SSR matters, an issue ICANN must address going forward to fulfil its SSR obligations.

Detailed Assessment

SSR1 Recommendation 1: ICANN should publish a single, clear and consistent statement of its SSR remit and limited technical mission. ICANN should elicit and gain public feedback in order to reach a consensus-based statement.

What was done to implement the recommendation? Was the recommendation fully implemented?

The team observes that a statement exists[2], and it was updated as a result of review by the community[3]. Despite the existence of this statement, the use of definitions remains inconsistent. For example, the definitions of Security and Stability contained in ICANN's agreements with contracted parties are different.

Did the implementation have the intended effect? How was the assessment conducted?

No metrics were provided to evaluate whether the implementation had its intended effect; however, available evidence indicates that the implementation did not have its intended effect.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

This recommendation remains relevant, and SSR2 had discussions regarding the development of a clear and consistent statement as well as how to get public feedback on such a statement. Further work is needed to bring this process to closure, especially because of the inconsistencies between different versions of the remit[4]. This recommendation remains relevant, and we propose a new recommendation on this topic later in this report.

SSR1 Recommendation 2: ICANN's definition and implementation of its SSR remit and limited technical mission should be reviewed in order to maintain

[2] https://www.icann.org/resources/pages/ssr-role-remit-2015-01-19-en

[3] https://www.icann.org/en/system/files/files/report-comments-ssr-rt-draft-report-18may12-en.pdf

[4] See, for example, clause 7.3 of the registry agreement updated on 31 July 2017 at https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.docx

consensus and elicit feedback from the Community. The process should be repeated on a regular basis, perhaps in conjunction with the cycle of future SSR reviews.

What was done to implement the recommendation? Was the recommendation fully implemented?

The review team noted a correlation between R1 and R2.[5] As pointed out above, the team observes that a statement exists, and it has been reviewed by the community. The use of definitions remains inconsistent. For example, the definitions of Security and Stability contained in ICANN's agreements with contracted parties are different. In recent years, updates to the SSR Framework have received community review, but this was not done for every update.

Did the implementation have the intended effect? How was the assessment conducted?

The implementation of this recommendation is incomplete, mainly because the concept of community input needs to be part of a clear framework that is adopted by community consensus.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

The recommendation is still relevant. Given the SSR activities and challenges that the ICANN community faces, further work is needed. Specifically, regular reviews of the SSR remit have not happened. There have been no opportunities to comment specifically on the remit and mission statement since 2013. Current definitions make it difficult to assess the implementation.

~~*RECOMMENDATION:*~~

~~Using a process that is aligned with the community review of the ICANN Strategic Plan and the ICANN Operating Plan, each time the SSR framework is updated or changed, the community should have an opportunity to comment on ICANN's definition and implementation of its SSR remit and limited technical mission.~~

[5] When referring to other recommendations, this scheme will be used throughout this document.

SSR1 Recommendation 3: Once ICANN issues a consensus-based statement of its SSR remit and limited technical mission, ICANN should utilize consistent terminology and descriptions of this statement in all materials.

What was done to implement the recommendation? Was the recommendation fully implemented?

The review team noted a correlation between R1 and R2. As pointed out above, the team observes that a statement exists, and it has been reviewed by the community. A blog post from July 2013 lists ICANN's security terminology available to the whole community; however, these definitions do not appear to be consistently integrated into other SSR-related documents. The use of definitions remains inconsistent. For example, the definitions of Security and Stability contained in ICANN's agreements with contracted parties diverge. Therefore, it is clear that the definitions of Security and Stability contained in ICANN's agreements with contracted parties are not completely consistent.

Did the implementation have the intended effect? How was the assessment conducted?

It is very likely that the implementation did not have its intended effect. ICANN's staff report on this recommendation indicates that staff would "add key terms to ICANN's public glossary on an ongoing basis as part of SOP; as SSR activities evolve, terminology and descriptions will be updated as part of SOP. However, the glossary has not been updated since February of 2014. Further, there are no references to SSR, its remit or mission in the publicly available glossary.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

The recommendation is still relevant. The team did not find procedures that are used to ensure that the defined terms are used in all material and communications; however, the team did find evidence of inconsistencies. Therefore, further work would include updating current definitions where needed, publicise them appropriately, and establishing procedures to ensure consistency. ICANN should develop a public glossary for the ICANN community, and then develop procedures that ensure the terms in the glossary are used in all material and communications, and revisited - and if necessary updated - on a yearly basis, with document control in place to make

changes trackable. This process should have an owner within ICANN Org who would also be responsible to provide clarification of terms when needed.

SSR1 Recommendation 4: ICANN should document and clearly define the nature of the SSR relationships it has within the ICANN Community in order to provide a single focal point for understanding the interdependencies between organizations.

What was done to implement the recommendation? Was the recommendation fully implemented?

ICANN reports that many SSR relationships have been defined and publicized.[6] As part of the OCTO SSR Team SOP, these are supposed to be updated periodically.[7] Memorandums of Understanding (MOUs) have been signed with numerous entities.[8] It was expected that SSR-related portions of these MOUs would be extracted and and catalogued; however, ICANN reports that some relationships are sensitive, and thus they are not disclosed. As pointed out above, the team observes that a statement of SSR-related roles and responsibilities exists, and it has been reviewed by the community.

Did the implementation have the intended effect? How was the assessment conducted?

The implementation did not have the intended effect. The key document for tracking ICANN SSR-related roles and responsibilities lists every organization with which ICANN has ever had a formal relationship, a pointer to the document that underpins that relationship, and a description of the SSR components of that relationship.[9] Many of the references cannot be located online. Furthermore, there are additional documents that provide small pieces of evidence rather than single focal point called for in the recommendation. In addition, the document often shows the SSR components of the relationships as “unknown.”

[6] https://www.icann.org/sites/default/files/assets/security-2000x1295-30jul13-en.png
[7] https://www.icann.org/en/system/files/files/is-ssr-update-s2-2014-21jan15-en.pdf
[8] https://www.icann.org/resources/pages/governance/partnership-mous-en
[9] https://www.icann.org/en/system/files/files/ssr-relationships-fy17-23jan17-en.pdf

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

This recommendation is still relevant today. Whenever questions about ICANN's SSR remit and relevant relationships arise, there should be a comprehensive and informative focal point for understanding SSR's relationships with other organizations in- and outside the ICANN community. Further work is needed to update the **document that defines the nature of the SSR relationships**. This document must be kept up to date. It should indicate what relationships exist, what aspects they cover, and how they are maintained in contrast to the current form where no indicative information is given for the majority of entries. If information is to be omitted in the public-facing document, information should still be filed.

SSR1 Recommendation 5: ICANN should use the definition of its SSR relationships to maintain effective working arrangements and to demonstrate how these relationships are utilized to achieve each SSR goal.

What was done to implement the recommendation? Was the recommendation fully implemented?

Reporting on ICANN's progress toward SSR-related critical success factors (CSFs) and key performance indicators (KPIs) involving SSR relationships is part of the OCTO SSR Team SOP, and they can be found in regular project management reporting, operating plans, the SSR Framework, and SSR quarterly reports.
The team expects the SSR Framework to include information on how the key relationships[10] called for in SSR1 Recommendation 4 are used to achieve SSR goals; however, this information is not readily available.

Did the implementation have the intended effect? How was the assessment conducted?

While evidence has been presented that ICANN has taken various steps to forge relationships, little evidence is available regarding what these relationships entail and whether they are effective. Therefore, the SSR2 team cannot assess if working relationships are functional. There is some evidence however, that ICANN has succeeded in establishing relationships with relevant actors.

[10] https://www.icann.org/en/system/files/files/ssr-relationships-fy17-23jan17-en.pdf

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

ICANN should be encouraged to do routine SSR reports and ensure that the sections related to relationships with other, external organizations are highlighted and kept up-to-date. Where possible, insight into these relationships should be provided in an easily accessible format. Lastly, the recommendation specifically mentions maintenance, making this is a constant process.

SSR1 Recommendation 6: ICANN should publish a document clearly outlining the roles and responsibilities for both the SSAC and RSSAC in order to clearly delineate the activities of the two groups. ICANN should seek consensus for this across both groups, recognizing the history and circumstances of the formation of each. ICANN should consider appropriate resourcing for both groups, consistent with the demands placed upon them.

What was done to implement the recommendation? Was the recommendation fully implemented?

The roles and responsibilities for SSAC and RSSAC are captured in a document.[11] However, this public document is still marked as "DRAFT UNDER REVIEW." If consensus was achieved, a final document could not be located.

ICANN uses the web site (https://www.icann.org/public-comments) to manage the public comment process. However, the web site does not capture information about calls for public comment in a way that is easy to search. It is especially difficult to gather history for public comments that happened many years ago. As a result, if consensus was ever achieved, a final document could not be located.

Did the implementation have the intended effect? How was the assessment conducted?

This recommendation was not implemented. The recommendation calls for a consensus document, and the documentation to related to the consensus process

[11] https://www.icann.org/en/system/files/files/draft-rssac-ssac-roles-responsibilities-05mar15-en.pdf

reached cannot be located. It appears that work was started on this recommendation; however, it concluded without addressing organizational reviews of SSAC and RSSAC.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

This recommendation remains relevant. ICANN should update the draft document from March 2015, and then the public comment should be resumed or repeated. ICANN should confirm agreement by RSSAC and SSAC, and initiate a public comment for this document that describes the roles and responsibilities for both the SSAC and RSSAC. If consensus is reached, produce a final document with a stable URL.

To facilitate the investigation after public comment is over, ICANN should create an email list or tracking tool for announcements about public comment. At least three messages should be sent to this mail 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. Finally, ICANN shall consider having a page dedicated to listing all public calls for comments which would then be linked to the page of the relevant document.

SSR1 Recommendation 7: ICANN should build on its current SSR Framework by establishing a clear set of objectives and prioritizing its initiatives and activities in accordance with these objectives.

What was done to implement the recommendation? Was the recommendation fully implemented?

The recommendation partly was implemented. It is apparent that the Strategic and Operating Plans were informed by the SSR Framework and include SSR priorities, objectives and activities. SSR-related activities are reported on regularly as part of

SOP, including in ICANN's regular portfolio management reporting[12] and SSR quarterly reports.[13] The process for updating SSR related documents has been redesigned, and the SSR mission and approach was published in 2015. However, there is a lack of community input and a clear framework of how strategy informs SSR activities.

Did the implementation have the intended effect? How was the assessment conducted?

Strategic planning for security, stability and resiliency issues appear to be centered on the Office of the CTO (OCTO), and it is apparent that a level of planning exists within the OCTO. However, the level of detail and planning envisioned in the recommendation does not seem to be provided in public discussions. Furthermore, there remains no obvious way for the ICANN community to provide input on the objectives, initiatives, and priorities of activities related to SSR beyond high-level documents.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

The recommendation is still relevant. Clear frameworks and objective setting are a key tool needed to attain security and resiliency goals. While specific and implementation-related planning is likely well-served by specialists, the community should be able to provide input into these key strategies, as they relate strongly to ICANN's core mission. Therefore, further work is needed.

~~*RECOMMENDATION:*~~

~~ICANN should formulate clear and measurable key objectives and strategies for SSR activities, update them regularly, attain community feedback, and publish the resulting documents. Then, these agreed principles should guide SSR activities throughout the community.~~

SSR1 Recommendation 8: ICANN should continue to refine its Strategic Plan objectives, particularly the goal of maintaining and driving DNS availability. Clear alignment of Framework & Strategic Plan.

[12] https://www.myicann.org/plan/
[13] https://www.icann.org/news/blog/identifier-systems-ssr-activities-reporting-en

What was done to implement the recommendation? Was the recommendation fully implemented?

The Strategic and Operating Plans (SOP) were informed by SSR Framework and reflect SSR priorities, objectives and activities. However, the SOP does not indicate which activities, priorities and expenditures in the SOP are SSR-related. Crucially, the mechanisms envisioned by SSR1 have been replaced by other organizational and process tools, complicating both assessment and implementation.

Did the implementation have the intended effect? How was the assessment conducted?

Available documents indicate that Security, Stability, and Resilience are included and addressed in relevant reports, strategies, and procedures. However, available reports do not provide sufficient insight into SSR activities and lack detail regarding the implementation and the execution of SSR activities. While advisory committees, namely SSAC and RSSAC exist, there is little opportunity for other parts of the community to provide input (or even learn about SSAC input) on the objectives, initiatives, and priorities of activities related to SSR.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

As with SSR1 Recommendation 7, the ICANN community has routine opportunity to comment and discuss priorities and objectives at a high level, as published in its strategic plan. The chief concern is the level of detail related to SSR activities. In the interests of transparency and accountability, the recommendation remains relevant today. However, the mechanisms envisioned by SSR1 for achieving this have been replaced by other organizational and process tools at ICANN. It would be useful to undertake more detailed and public objective setting with prioritization done via public, community input processes. Furthermore, these objectives would have to be written in a way that allows them to feed into applicable and measurable SSR activities.

~~*RECOMMENDATION:*~~

~~It is recommended that the process used to develop the SOP should include more community involvement in SSR matters, and should provide procedures in setting the objectives and prioritization at more detailed level than is done today.~~

Revisit for general recommendation on community integration

SSR1 Recommendation 9: ICANN should assess certification options with commonly accepted international standards (e.g. ITIL, ISO and SAS-70) for its operational responsibilities. ICANN should publish a clear roadmap towards certification.

What was done to implement the recommendation? Was the recommendation fully implemented?

This recommendation was not fully implemented. ICANN has pursued some certifications focussed on IANA, e.g. SOC2/3 Certification of Root Zone KSK System, and SOC2 Certification for the Registry Assignment and Maintenance Systems, and SysTrust for the implementation of DNSSEC at root level. Outside of the IANA functions, ICANN reports using continuous improvement frameworks in IT and cybersecurity, has an annual financial audit, performs an annual EFQM self-assessment and documentation review, and obtains professional advice to help measure performance and drive improvement. ICANN also reports that all information security staff are trained using SANS offerings. Lastly, ICANN reports that the outcomes of internal audits are reported to the Board only. Thus, ICANN has not published a document that could be used as a roadmap for SSR process certification, making community review impossible. Therefore, it is not obvious how ICANN assessed certification options as a result of SSR1. In any case, ICANN has not published “a clear roadmap towards certification.”

Did the implementation have the intended effect? How was the assessment conducted?

While ICANN has undertaken some steps towards certification, a clear roadmap and an overarching strategy is not apparent. This conclusion was reached by assessing publicly available material and submitting questions to ICANN staff. At this point in time, ICANN Org has undertaken various steps towards training staff, and in some cases pursued organisational certifications. While the recommendation calls for a “clear roadmap”, there is no evidence available publicly or to the review team that

such a roadmap has been created. ICANN Org seems to follow an ad hoc approach, rather than organising and tracking its activities in this area. Besides, ICANN has not followed industry best practice, e.g. by not rotating auditors on a regular basis, and has failed to demonstrate that all certification activities feed into relevant risk and information security frameworks and strategies.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

While ICANN runs specific infrastructure that some standards might struggle to capture appropriately, there is value in pursuing individual and organisational certifications, particularly if these goals are organised and planned appropriately. Therefore, this recommendation is still relevant, and further work is needed. ICANN can, and 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 and report on their procedure and the standards' suitability. ICANN should publish a clear roadmap towards achieving relevant certifications.

RECOMMENDATIONS:

ICANN should fully implement the initial SSR1 Recommendation 9, as certification is possible and adequate. In particular, establish a road map of what certification activities are being undertaken and what certifications ICANN is aiming to achieve. ICANN should also provide reasoning for their choices, demonstrating how they fit into its 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. For example, ICANN Org should explain which certifications or trainings are relevant to which roles in the organisation, and track completion rates.

SSR1 Recommendation 10: ICANN should continue its efforts to step up contract compliance enforcement and provide adequate resources for this function. ICANN also should develop and implement a more structured process for monitoring compliance issues and investigations.

There is no doubt that ICANN's compliance function has stepped up considerably since 2011, when the SSR1 recommendations were made. ICANN now produces monthly reports about its compliance enforcement work. However, it is not clear the extent to which SSR issues are handled within the compliance process. Note that more than 80% of complaints against registrars in August 2018 related to WHOIS inaccuracy.

What was done to implement the recommendation?

The SSR1 implementation report is available here (slides 28-30) and the SSR2- RT briefing on this recommendation is available here. Regular public reporting of compliance activities is part of ICANNs SOP. To support this, ICANN has a dedicated public page for Contractual Compliance Reporting including data on monthly, quarterly and annual data, 10 different reports quarriable over a 13-month period, and metrics and data specifically requested by different working groups. Some Compliance auditing and outreach programs are now in place. To address resources, new positions in ICANN were created after the SSR1 Review to ensure fulfillment of goals and objectives in this area.

Complaints mechanisms were updated by migrating to icann.org, automating, and launching a bulk complaint tool. Additionally, a Pulse Survey was implemented. With specific respect to WHOIS, an inaccuracy qualities check was launched. WHOIS accuracy reporting has been underway since the 2012 WHOIS Review Team recommended the action.

While acknowledging the efforts made, there still is work to be done to fully implement this recommendation. For instance, compliance enforcement reports for 2017 and 2016 contain little evidence of SSR enforcement actions. However, the new gTLD base registry agreement (July 2017) contains specific obligations on contracted parties relating to security and stability and may assist further implementation. It still remains unclear how ICANN's goal to reduce the incidence and impact of registration abuse and malicious conduct carries through compliance actions or other initiatives. The majority of the issues in the staff SSR1 implementation report highlight matters relating to WHOIS. Additionally, the registrar agreement (RAA 2013) contains vague enforcement rights for ICANN in relation to registrars whose operation endangers Registrar Services, Registry Services or the DNS or the Internet.

Was the recommendation fully implemented?

No, it was partially implemented.

Did the implementation have the intended effect? How was the assessment conducted?

Since 2011 ICANN's compliance has professionalized and there is greater transparency about its work through the provision of monthly reports. However, it is not clear the extent to which SSR issues are handled within the compliance process.

Despite other requirements for Compliance improvements, such as those arising from the first WHOIS Review, and the ATRT first and second report advocating a strengthening of ICANN's compliance function, much improvement work remains to be done.

How was the assessment conducted?
The assessment is based on publicly available information (e.g. the Contractual Compliance Reporting page) as well as an ICANN staff report which provided evidence of implementation of the recommendation.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

Yes, this continues to be relevant. Further work would be to drill down into greater detail on specific security, stability and resilience issues – such as those outlined in ICANN's SLA monitoring system, along with details on follow-up and any enforcement action.

Recommendation on Compliance and Enforcement

SSR1 Recommendation 11: ICANN should finalize and implement measures of success for new gTLDs and IDN fast track that expressly relate to its SSR-related program objectives, including measurements for the effectiveness of mechanisms to mitigate domain name abuse.

What was done to implement the recommendation? Was the recommendation fully implemented?

No measures for success, including measurements for the effectiveness of mechanisms to mitigate domain name abuse have been defined in a document that has community consensus. This has also been noted in the recent CCT's report and recommendations[14]. It appears that despite the new gTLD and IDN fast track programs having been in existence (or advance planning) since the SSR1 report was published, it appears that SSR objectives required by SSR1 Recommendation 11 remain 'to be defined'.

Nevertheless, some important things have been done to mitigate domain name abuse, including: the Public Safety Working Group (PSWG) was formed in 2015 to focus on abuse of and within the DNS ecosystem and foster collaboration amongst registries, registrars, cyber security, and law enforcement, and the DAAR system has been proposed to report on abuse trends across gTLDs and a number of abuse types (unfortunately, as of this writing, it still has not been published).

Furthermore, specification 11 of the new Registry Agreement contains substantial SSR obligations on registries including obligations to periodically conduct a technical analysis and maintain statistical reports to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. These exact obligations have been part of the standard new gTLD registry agreement since applications opened in 2012. Unfortunately, no metrics for evaluating compliance to these obligations appear to exist.

Security and stability reviews under the IDN ccTLD Fast Track process have been ineffective. All applications that have passed through the security and stability panel have been found not to create a technical SSR risk. The EPSRP mechanism in the staff report has been criticized by community members and ICANN staff as expensive and ineffective.

Did the implementation have the intended effect? How was the assessment conducted?

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. No measures for success, including measurements for the

[14] https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf

effectiveness of mechanisms to mitigate domain name abuse, have been defined in a document that has community consensus.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

The DNS landscape has changed since the first SSR review team made its recommendations as a result of the new gTLD expansion in particular. However, the recommendation to embed SSR considerations as a key measure of success in the management of the DNS space remains just as relevant, if not more so, today as it was in 2011.

RECOMMENDATION:

Coordinated vulnerability disclosure reporting would be an excellent project for ICANN to progress. It is difficult to assess the status of this initiative as the link included in the staff report goes to a document from 2013. Also a clear communication plan on how it reports this to the community-at-large would be a useful tool as well.

SSR1 Recommendation 12: ICANN should work with the Community to identify SSR-related best practices and support the implementation of such practices through contracts, agreements and MOUs and other mechanisms.

What was done to implement the recommendation? Was the recommendation fully implemented?

Recommendation 12 appears to have driven ICANN's SSR Team - now ICANN's OCTO SSR Team - to continue to build their engagement both on an individual networking level, and to engage heavily with ICANN's GSE Department (Global Stakeholder Engagement). The OCTO Team has worked with GSE since this recommendation.

While SSR-related interactions with SOs and ACs are documented through the regular ICANN processes, they are not specifically flagged in any way beyond meetings at ICANN being labelled as of interest for those in the community with a security interest. One such effort could be OCTO SSR team member participation in the ccNSO TLD-OPS discussions list but, once again, these are not documented by OCTO SSR.

In the Identifier System Attack Mitigation Methodology paper, the SSR2 Review Team found a non-exhaustive list of attacks against the Identifier System that has been put forth for consideration within ICANN. Although there have been some agreements/renewals/specifications/MOUs since February 2017, nothing specifically from that paper has ever been included in the contracts with contracted parties.

Was the recommendation fully implemented?
No.

The report entitled "Identifier System Attack Mitigation Methodology" is dated February 2017. The paper sets out suggestions said to have been generated 'within ICANN and by Identifier System security experts throughout the Community.' However, it is not clear what process was followed in arriving at the best practices set out in the document. In any event, there is no evidence in the linked-to paper of any integration of those best practices into agreements into which ICANN enters. There is no evidence of work prior to 2017 contained in the report.

The resource locator page linked to has not been updated since 2014. The 'additional information' links to the SSR annual reports page (which does not mention best practices, at least on its face), and the other link does not resolve.

SSR2's review found no evidence of staff periodically informing SO/ACs of best practices, or inviting them to identify additional best practices.

Another deliverable is that staff is to address SSR-related responsibilities and best practices in Regional Engagement Strategies. In examining the ICANN Engagement Strategy in the Middle East a single action is related to SSR initiatives: conducting contingency and coordination exercises to prepare for threats to DNS and prepare CERTs. In the Latin American and Caribbean Strategy document only action 2.2.1 (a roadshow) is related to SSR. In the African Strategic Plan, two strategic projects touch on SSR: project 2,

The staff report on this SSR1 recommendation indicates that work with the Anti-Phishing Working Group Internet Policy Committee on publishing recommendations for web application protection and development of resources for security awareness is complete. There is an advisory from APWG on "What to Do if Your Website Has Been Hacked by Phishers," but it was produced prior to SSR1. Other than Phishing Trends Surveys and Reports, APWG does not seem to have

released a new recommendation or report from its Internet Policy Committee. While there is a report from the 4th Global DNS Stability, Security and Resiliency Symposium held in Puerto Rico in 2012, the ICANN web site does not appear to have a set of recommendations for web application protection and development of resources for security awareness.

Did the implementation have the intended effect?
This SSR1 Recommendation has had partial implementation through the accumulation of other initiatives in OCTO. It is not apparent that any attempt was made to implement the specific goals of this Recommendation.

In addition, Specification 11 of the new Registry Agreement (RA) contains substantial SSR obligations on registries. The obligations in this RA have been part of the standard new gTLD registry agreement since applications opened in 2012. However, ICANN has apparently not used these provisions as a baseline for assessing how effective they are in meeting the goals of SSR1 Recommendation 12.

How was the assessment conducted?
The assessment was conducted by reviewing the briefing materials provided by staff, interviews with staff, and following links to supporting materials. It should also be notes that, while the SSR2 team identified activities that are relevant to SSR-related best practices, the SSR2 team did not undertake a concerted, documented effort to work with the community to identify and implement SSR-related best practices.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

This recommendation remains relevant today, if not more so. Cybersecurity threats are becoming more acute and several countries are now adopting specific cybersecurity strategies. Maintaining and improving the security, stability and resilience of the domain name system is a limited but essential part of ensuring the security and stability of the entire network.

Further work is needed to fulfil the objectives of the recommendation and bring ICANN forward to a proactive position in working through the community to improve SSR.

RECOMMENDATION:

ICANN should work with the Community to identify SSR-related best practices, and then implement the practices through contracts, agreements, MOUs, and other mechanisms. {{Make measurable}}

SSR1 Recommendation 13: ICANN should encourage all Supporting Organizations to develop and publish SSR-related best practices for their members.

What was done to implement the recommendation? Was the recommendation fully implemented?

ICANN considers work on this recommendation ongoing, and reports that as part of SOP, ICANN staff contacts all SOs and ACs to encourage identification and publication of a best practices repository page. ICANN reports further that their staff engages in a variety of ongoing activities to encourage global use of SSR best practices, as part of SOP. The review team cannot assess if these recommendation was implemented, as there is no available evidence whether this was done or not. Responding to questions from the review team, staff reported that they were not aware of any recent steps that have been taken to encourage SOs and ACs to produce and publish best practices repositories for SSR-related information.[15] Moreover, as answer to one of the questions provided to the staff, they reported that only ccNSO currently publishes the SSR-related best practices for their members.

The RT also notes that the recommendation is not measurable as it is not possible to measure the extent to which ICANN encouraged its SO/AC to develop and publish SSR-related best practices.

Did the implementation have the intended effect? How was the assessment conducted?

No. Only one example of successful publication exists. This was in 2012.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

[15] Stating that "it is likely that the 2012 information on the ccTLD website may be the most recent example of SSR-related information published by a Supporting Organization."

Yes, this is still relevant because SSR objectives need to be followed and applied throughout to be effective.

The RT recommends ICANN to develop a concise a consistent process that helps all SO/AC to develop and implement a consistent model for publishing SSR-related best practices. ICANN should document and report all such efforts made in this respect.

Recommendation:

~~ICANN should adopt a general SSR policy and strategy, which requires SOs to discuss and implement relevant aspects, and make available relevant information to their constituents.~~

SSR1 Recommendation 14: ICANN should ensure that its SSR-related outreach activities continuously evolve to remain relevant, timely and appropriate.

What was done to implement the recommendation? Was the recommendation fully implemented?

The Engagement Interface (https://features.icann.org/events-near-you) did not directly address how the outreach activities "evolve" to remain relevant. The implementation focused, instead, on reporting what is being done at any given time. As the focus on evolving activities is not being addressed, the recommendation has not been implemented.

Did the implementation have the intended effect? How was the assessment conducted?

No. The reported implementation of this recommendation did not directly address how the outreach activities "evolve" to remain relevant. The implementation focused, instead, on reporting what is being done at any given time.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

This recommendation remains relevant. The SSR communities are a non-stationary set and are always evolving, and staying in-step and plugged in with them is critical.

Having some machinery in place that tracks communities and assesses their relevance to ICANN's SSR is an important ongoing activity that does not appear to be addressed.

SSR1 Recommendation 15: ICANN should act as a facilitator in the responsible disclosure and dissemination of DNS security threats and mitigation techniques.

What was done to implement the recommendation? Was the recommendation fully implemented?

ICANN has implemented a Vulnerability Disclosure Program for ICANN's public-facing assets. When vulnerabilities against DNS infrastructure are reported to ICANN, ICANN when feasible disseminates to responsible external third-parties. However it is the responsibility of the third-party to remediate any vulnerability within their platform(s). Furthermore, since 2013, none of the IS-SSR reports contain any statistics or metrics related to disclosure reporting. It is impossible to tell from published materials if the vulnerability disclosure reporting methodology has ever been invoked, or if it is functional. No data, even in anonymized form, is available about ICANN as a vulnerability coordinator, its work in emergency coordination and SSR-related crisis management. As a result, it is impossible to tell – from available, information – whether or not this recommendation has been implemented.

Did the implementation have the intended effect? How was the assessment conducted?

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. Therefore, while a process exists "on paper", it is not possible to assess if that process is functional and effective.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

The motivations behind SSR1 Recommendation 15 remain relevant today. The SSR2 team considers it necessary for ICANN to provide an appropriate and proportionate level of insight into the vulnerability disclosure process and its efficacy.

Recommendation:

ICANN should provide anonymised metrics of the vulnerability disclosure process on a regular and timely basis.

SSR1 Recommendation 16: ICANN should continue its outreach efforts to expand Community participation and input into the SSR Framework development process. ICANN also should establish a process for obtaining more systematic input from other ecosystem participants.

What was done to implement the recommendation? Was the recommendation fully implemented?

There is ongoing outreach by ICANN to related communities, which accomplishes the "participation" objective. However, the recommendation requests outreach to additional SSR communities. There is no evidence that current outreach activities have resulted in expanded Community participation. There is no evidence of a process for "systematic[ally]" incorporating other ecosystem participants. Furthermore, the recommendation specifically asks for a more systematic process for getting input from other ecosystem participants. This makes the final deliverable seem out of place. The Implementation Report says that staff would "support a variety of capability building initiatives by the Security Team." It is not immediately evident how these capability building initiatives would affect greater engagement in the development of the SSR Frameworks or Annual Reports. It is also not obvious from the public record what those capability building initiatives were or when they were conducted.

Did the implementation have the intended effect? How was the assessment conducted?

This recommendation was partly implemented. It seems that the ongoing involvement in related communities has accomplished the "participation" objective, but it is not clear how information is "systematic[ally]" incorporated. This recommendation envisions greater public engagement with SSR initiatives, including the Frameworks and Annual Reports. This recommendation resulted in no obvious changes to the way the SSR Framework and Annual Reports are created. It is not immediately obvious how changes to the organization or processes related to SSR activities have expanded participation and input.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

This recommendation remain relevant. The SSR space is very non-stationary and needs to both be kept up with, and interacted with. Relevant actors to engage with are appearing regularly and should be reached out to.

Recommendation:

ICANN needs to develop an overarching SSR strategy that includes measurable or trackable objectives pertaining to the acquisition of external feedback and outreach to relevant non-community as well as community stakeholders. This should incorporate some of the observations made under the review of previous recommendations.

SSR1 Recommendation 17: ICANN should establish a more structured internal process for showing how activities and initiatives relate to specific strategic goals, objectives and priorities in the SSR Framework.

What was done to implement the recommendation? Was the recommendation fully implemented?

The implementation report refers to the deliverables in Recommendation 2 as a guide to how recommendation 17 was implemented. However, Recommendation 2 and 17 have different goals. Recommendation 2 asks that the SSR-related activities and remit go through regular public consultation. Recommendation 17 suggests that SSR-related initiatives relate to specific strategic goals, objectives and priorities. The deliverables for Recommendation 2 do not meet the requirements of Recommendation 17.

The most recent Annual Report lists eighteen separate initiatives for the fiscal year and then describes how those initiatives connect to the overall mission of the Office of the CTO and ICANN's overall strategic plan. The Annual Plan then links to activity reports that describe the work completed in a reporting period (six months).

The connection between the SSR Annual Report and ICANN's Strategic Plan is not obvious. Furthermore, the Strategic Plan does not mention the SSR Annual Reports and barely mentions SSR-related activities. If a more structured internal process for showing how activities and initiatives relate to specific strategic goals, objectives and priorities in the SSR Framework is present, it is not available publicly or to the review team. However, the section of the most recent Annual Report which identifies annual initiatives does attempt to relate them to ICANN's Strategic Plan.

Did the implementation have the intended effect? How was the assessment conducted?

Other SSR1 Recommendations attempt to align and integrate ICANN's SSR activities with the overall Strategic Plan. The implementation of SSR1 Recommendation 17 falls well short of providing a structured and easily reviewed internal process. Due to a lack of trackable indicators, the status of implementation is impossible to ascertain from publicly available materials.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

Clear processes for SSR-related issues remain relevant. Like other SSR1 Recommendations where the target was greater community participation in the development of objectives and priorities, SSR1 Recommendation 17 requires better metrics for evaluating the success of the implementation, processes for community integration and feedback, and finally a clear relation to strategic plans, policies, and goals.

SSR1 Recommendation 18: ICANN should conduct an annual operational review of its progress in implementing the SSR Framework and include this assessment as a component of the following year's SSR Framework.

What was done to implement the recommendation? Was the recommendation fully implemented?

On the surface, this has been completed annually except for FY15-16. The team cannot assess the status of FY18, since it is not yet on the web site. However, SSR1 Recommendation 18 suggests a recursive approach where the review of a previous

year's activity will influence the decisions about the initiatives in a future year. While this may be taking place informally, there is no public reporting or mechanism for input on a SSR-related operational review.

Did the implementation have the intended effect? How was the assessment conducted?

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.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

SSR1 Recommendation 18 should be reconsidered and reissued in a form that can be effectively assessed in the future. As in other cases, a future implementation must be measurable.

SSR1 Recommendation 19: ICANN should establish a process that allows the Community to track the implementation of the SSR Framework. Information should be provided with enough clarity that the Community can track ICANN's execution of its SSR responsibilities.

What was done to implement the recommendation? Was the recommendation fully implemented?

ICANN Org reports that The publication of the annual SSR Framework[16] tracks progress against the activities committed to in the previous year's Framework. Additionally, regular project management reporting, and operating plans and budgets, are considered tools that provide details on SSR activities. However, publishing an annual SSR Framework on the website does not seem to serve the purpose of informing the community and allowing them to track the implementation of the framework. Documentation of the implementation lags very much behind the implementation, so it does not offer the Community a way to track the SSR-related activities. Moreover, it appears that the SSR1-RT provided an example to have a public dashboard for tracking the SSR-related activities, as was done to implement

[16] https://www.icann.org/ssr-document-archive

one of the recommendations of ATRT. However, there is no evidence that such dashboard is available to community or public for SSR-related activities.

The RT also notes that the recommendation 19 suggested to provide information with "enough clarity". However, this does not seem to be measurable in its entirety.

Did the implementation have the intended effect? How was the assessment conducted?

The RT realizes that there may be data available that could be used to support the implementation of recommendation 19. But the formal process was never initiated in this regard except publishing the annual SSR framework. Hence, RT concludes that the intended effect has not been achieved since there currently is no mechanism to track the implementation of the SSR Framework effectively.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

As in other SSR1 Recommendations, this remains relevant for the purposes of transparency and accountability of the ICANN Organization. As with a number of other SSR1 Recommendations, a functional procedure and reporting structure needs to be developed and implemented with community feedback, and should be accessible to the community.

SSR1 Recommendation 20: ICANN should increase the transparency of information about organization and budget related to implementing the SSR Framework and performing SSR-related functions.

Annual reporting on SSR-related activities is included in the Framework documents and Annual Reports. Budget documents have very high-level line items to activities related to SSR. However, those same activities do not appear to be reported on in ICANN's regular project management reporting. The staff implementation report says that ICANN will "Integrate SSR Framework and reports on SSR activities and expenditures into planning framework and process to provide public information about SSR-related plans, budgets and activities." However, as noted for Recommendation 19, the ICANN Portfolio Management System and the KPI Project Dashboard have very limited amounts of information that the Community can use to track SSR-related efforts.

The FY 2018 approved budget has three portfolio areas related to SSR[1]: Identifier Evolution, Security, Stability, and Resiliency of Internet Identifiers, and Technical Reputation. Unfortunately, only the first two (Identifier Evolution and SSR of Internet Identifiers) have dedicated budgets at the portfolio level and no detail of these budgets is provided. The staff implementation report also says that ICANN will "Identify mechanisms that provide more detailed public information on SSR-related budgets and expenditures across multiple ICANN departments", indicating a further work is needed on this aspect of implementation.

What was done to implement the recommendation?

The SSR1 implementation report is available here (slides 58-60), and the SSR2-RT briefing on this recommendation here (slides 30-37). Work was done in two phases.

Phase I included a planning framework and process now in place to provide public information about SSR-related plans, budgets and activities (as outlined in Recommendation 2). This is integrated with ICANN's SSR Framework and reports on SSR activities and expenditures. Periodic SSR activity reporting augments this public information. Phase II is underway to identify mechanisms that provide more detailed public information on SSR-related budgets and expenditures across multiple ICANN departments. Currently, public information on this topic for FY18 can be found here.

Staff also developed an after-event-report that includes budget and resource impacts related to managing an event. No after-event reports have been published yet, although they should be published annually starting FY18. A template for a public version of these reports can be found here. ICANN also publishes an information security event log here.

ICANN reported that the Department spending on EBERO for FY17 totalled $2.3m and supported work on the following items: data escrow services ($930k); WHOIS studies (ARS design/analysis, parsing, accuracy testing, ARS phase 3; $638k); EBERO services ($353k); Background checks for registrar accreditation ($100k); and miscellaneous or smaller items ($300k)

As seen here, annual reporting on SSR-related activities does take place in the Framework documents and Annual Reports. However, the very high-level budget line

items should be accompanied by greater specificity and inclusion in ICANN's regular project management reporting to improve transparency.

Was the recommendation fully implemented?
No, it was partially implemented.

Did the implementation have the intended effect? How was the assessment conducted?

SSR related activities do appear in ICANN's annual budget, but at a very high level. SSR1's Recommendation 20 seems to have intended a greater degree of granularity for examination and public comment on SSR related budget items. The implementation did not have the full, intended effect. The assessment was conducted based on publicly available information, the SSR1 implementation report and SSR2 briefing.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

For the purposes of transparency and accountability, the recommendation continues to have relevance today.

RECOMMENDATION:

ICANN should increase the transparency of information about organization and budget related to implementing the SSR Framework and performing SSR-related functions.

SSR1 Recommendation 21: ICANN should establish a more structured internal process for showing how organization and budget decisions relate to the SSR Framework, including the underlying cost-benefit analysis.

This is very similar to Recommendation 20. In the staff implementation report there are three deliverables mentioned:

- Integration of the SSR framework and reports into the planning framework and process to provide public information about SSR-related plans, budgets and activities;
- Identification of mechanisms that provide more detailed public information on SSR-related budgets and expenditures across multiple ICANN departments; and,
- Exploration after event reports that include budget and resource impact related to managing the event.

The SSR! findings about the budget process made in Recommendation 20 above are equally applicable here.

The staff report specifically mentions a report template for publishing information related to budgets and resources impacted by security events. The link to the template does not resolve. The staff report suggests that this will be published annually every fiscal year, starting in FY18. An examination of SSR related pages on the ICANN website indicates that no report as, as yet, been published.

What was done to implement the recommendation?

Annual reporting on SSR-related activities does take place in the Framework documents and Annual Reports. The budget document has some very high-level line items to activities related to SSR. However, those same activities do not appear to be reported on in ICANN's regular project management reporting. This observation is the same as in SSR1's findings for Recommendation 20. In addition, the reporting on budget and resource impacts of SSR events appears to have never been done and the template for supporting that reporting does not appear to be available for public review or comment

Was the recommendation fully implemented?

ICANN's planning process ensures that activities planned and budgeted for, including those related to SSR, are identified by specific objectives. There has been no plan for getting public comment on the template being used for publishing more detailed public information on SSR-related budgets and expenditures. In fact, the template now appears to have been replaced by the annual report for the fiscal year.

The SSR1 Recommendation calls for a more structured internal process for showing how organization and budget decisions relate to the SSR Framework, including the underlying cost-benefit analysis. While there is more information available, the goal of the SSR1 Recommendation was a mechanism for showing, specifically, how organizational and budgetary decisions relate to the SSR Framework. This has either not been done or is not visible to the ICANN Community.

Did the implementation have the intended effect?

While there is more information available about ICANN's planning and budget process available, the call for a structured internal process for showing how organization and budget decisions relate to the SSR Framework, including the underlying cost-benefit analysis is not visible to the community. As a result, the Recommendation did not have its intended effect.

How was the assessment conducted?

The SSR2 team examined the publicly available records related to budget and activities in the SSR team – both under OCTO and prior to that office being established. The SSR2 team also examined materials prepared for SSR2 by staff in response to questions raised during the evaluation of SSR1 implementation. Finally, the SSR2 team reviewed briefings on the ICANN planning process and the objectives in the current strategic plan related to SSR at ICANN.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

As with recommendation 20, for the purposes of transparency and accountability, the recommendation continues to have relevance today.

SSR1 Recommendation 22: ICANN should publish, monitor and update documentation on the organization and budget resources needed to manage SSR issues in conjunction with introduction of new gTLDs.

This is a very similar to SSR1 Recommendations 20 and 21. The difference is that the documentation requested is the budget, resources and activities related to SSR

impacts of the new gTLD program. The staff report simply echoes the previous deliverables (for Recommendations 20 and 21) without providing any evidence or any specific work related to the new gTLD program. Thus, in the staff report for implementation, there is no new information that would help determine if the Recommendation was implemented.

It's clear that organization and budget for SSR issues related to the new gTLD team was provided via the Security team, but also reflected in the budget and organization for the new gTLD program (e.g., DNS Stability Panel, EBERO, other process steps, etc). It appears that the desired outcome of the implementation of this recommendation was to improve the amount and clarity of information on the organization and budget for implementing the SSR Framework and performing SSR-related functions related to the new gTLD program.

In the ICANN IS-SSR Document Archive there is no document that is specific to the new gTLD program. Examining the framework documents and Annual Reports, In the September 30, 2016 Framework, gTLDs are mentioned twice, once in Module A as a trend in the Internet ecosysystem and second, in Module B as part of the overall ICANN Strategic Plan. In the previous Framework, published in March 2013, the new gTLD program is again mentioned as a "trend," and as a policy driver for the gNSO. The only remaining mentions of the new gTLD program are in the section reporting on implementation of the SSR1 Recommendations.

What was done to implement the recommendation?

Public information on SSR-related budget and expenditures across multiple ICANN departments was posted for FY18 and can be found here: https://community.icann.org/x/DqNYAw. This report is updated annually and covers direct costs resulting from the activities required to perform the SSR Functions, direct costs of shared resource and the costs of support functions allocated to SSR. This report does not provide a breakdown of funding, resources or other activities related to the new gTLD program.

ICANN has also explored mechanisms that provide more public information on SSR-related budgets and expenditures across multiple ICANN departments. However, a template for that public information does not break out SSR activities or budgets related to the new gTLD program.

Was the recommendation fully implemented?
It was not.

Did the implementation have the intended effect?
It did not.

How was the assessment conducted?
The SSR2 team examined the publicly available records related to budget and activities in the SSR team – both under OCTO and prior to that office being established. The SSR2 team also examined materials prepared for SSR2 by staff in response to questions raised during the evaluation of SSR1 implementation.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?
Like recommendations 20 and 21, for the purposes of transparency and accountability, the recommendation continues to have relevance today.

RECOMMENDATION:

ICANN should publish, monitor and update documentation on the organization and budget resources needed to manage SSR-related issues in conjunction with introduction of new gTLDs.

SSR1 Recommendation 23: ICANN must provide appropriate resources for SSR-related Working Groups and Advisory Committees, consistent with the demands placed upon them. ICANN also must ensure decisions reached by Working Groups and Advisory Committees are reached in an objective manner that is free from external or internal pressure.

What was done to implement the recommendation? Was the recommendation fully implemented?

The SSR1 report provided only examples of SSR-related WGs (the Board DNS Risk Management Working Group and the DSSA-WG. It also provided examples of two SSR-related Advisory Committees: SSAC and RSSAC.

The DSSA-WG no longer exists, but there is a final report for this group.[17] Section 4 of that report talks about planned steps for the next phase of this work, which it is not clear happened. It is not clear whether they had appropriate resources. The rest of this commentary will restrict itself to SSAC and RSSAC.

ICANN does provide ICANN technical support staff to the SSAC and RSSAC to assist with writing documents. ICANN's budget include some funding to support SSAC and RSSAC to conduct meetings (travel expenses, hotel, food); ICANN pointed us at the 2015 budget as an example.[18] The support funding has never been linked to, or conditioned by, any formal performance/output/content evaluation. ICANN believes this enables adequate independence. In practice, it is not clear how RSSAC's or SSAC's work priorities are determined or evaluated by ICANN or the community, which creates an accountability gap, in addition to making it impossible to evaluate whether they have resources "consistent with the demands placed upon them" (by whom?). The original (2012) SSR1 report included the following text associated with this recommendation:

In discussions with the SSAC, it became apparent that at times they felt pressure to deliver an answer to specific problem within a very limited timeframe. This led to a shorter time period to evaluate the issue and more targeted recommendations as a result. Clearly, there will be times, when looking at immediate risks, that a timeframe is enforced upon research work. This is unavoidable. It would be prudent, however, to ensure that with proper planning, the SSAC and RSSAC are given as much time as possible to provide high-quality research work and findings.[19]

This observation precisely echos circumstances and concerns over the last couple of years, especially this year in the context of the KSK roll, during which SSAC struggled to be responsive to requests for advice on short time frames with inadequate data/research available to inform debate. It is likely that the fraction of ICANN's budget directed to SSAC is inadequate given many prevailing and emerging SSR issues and expectations that SSAC deliver advice that requires research or synthesis of other research. But the current structure of SSAC is also not compatible with "high-quality research work", since it is composed of a set of "volunteers", mostly from industry being subsidized by their employer for their time to participate (and thus not "free from external pressure"). The SSR2-RT does not believe that just throwing

[17] https://ccnso.icann.org/sites/default/files/filefield_42587/dssa-final-08nov13-en.pdf
[18] https://www.icann.org/en/system/files/files/adopted-opplan-budget-fy15-01dec14-en.pdf
[19] https://www.icann.org/en/system/files/files/final-report-20jun12-en.pdf

budget at the problem is sufficient to address this concern; rather, it will require a rethinking of the structure and expectations of not just these committees, but of ICANN itself.

A concrete example is the recent NCAP activities, where SSAC proposed a $3M budget to outsource some research they thought would be needed, which the ICANN Board thought was too expensive, or at least did not have sufficient justification, because SSAC had not performed a gap analysis from previous studies, which itself is research that requires resources that SSAC does not have. In the case of NCAP, the work also required a level of independence that SSAC did not have, since most members of the WG were in some way financially conflicted with the new gTLD program. Contributing to the challenge is the fact that ICANN's approach to self-managing conflict of interest is transparency, i.e., publishing "Statements of Interest", rather than follow a formal conflict-of-interest policy. This structure compromises the integrity of the work products since the balance of participation is weighted toward organizations with sufficient capital and financial incentive to participate, and there are no formal checks and balances to compensate.

The lack of metrics and monitoring of success or failure of the new gTLD program indicates this multi-stakeholder approach is not "free of external pressures". The CCT RT report on DNS abuse in new gTLDs has found metrics to rigorously apply, through which it is impossible to conclude that the gTLD program has been successful from a CCT perspective. Such research falls well within the roles and responsibilities of ICANN's Security Team (See SSR1 Recommendation 24). ICANN did not undertake or fund this sort of exercise itself, likely because external pressures against this sort of SSR research activity prevailed.

The review team also notes that there is nothing in the SSAC operational procedures document about managing external and internal pressures, except Section 2.1.2 Withdrawals and Dissents, which means each member, and the committee itself, self-manages conflicts of interest, and deliberations are all confidential for security reasons. The same appears true for RSSAC and RZERC, but in these two cases, the committees are architected such that each person represents a stakeholder. This structure is not a reliable recipe for ICANN to be in a position to "ensure" decisions are made in an objective manner free from external or internal pressures. ICANN staff do participate on the SSAC and RSSAC, which provides visibility into the committee dynamics and an opportunity to identify and attempt to mitigate such pressures. It also bears noting that important stakeholders are consistently missing from these

SSR2-related advisory committees: victims of identifier abuse, academic researchers, law enforcement, policymakers. This gap is not intentional, but it is by the nature of the charters of these groups, and it does affect the balance of pressures from various stakeholders.

With respect to RSSAC, a review of RSSAC's operations occurred in 2017-2018 in accordance with ICANN's bylaws, that also raised questions about RSSAC's accountability. The final report includes several recommendations relevant to this recommendation:[20]

> *Recommendation 2*
>
> *Resolve the apparent mismatch between the charter and operational procedures of the RSSAC and the requirements and expectations of the ICANN Board and Community for interaction with the root server system.* (The report footnotes that *"the publication of RSSAC037, "A Proposed Governance Model for the DNS Root Server System" ,*
> *(https://www.icann.org/resources/files/1216341-2018-06-15-en), is a clear and welcome first step in the direction suggested by this Recommendation."*)
>
> *Recommendation 3*
>
> *Formalize the responsibilities of the RSSAC to the ICANN Board and Community in a work plan that is periodically reviewed and published, and hold the RSSAC accountable for work plan deliverables.*
>
> *Recommendation 6*
>
> *Clarify the role and responsibility of the RSSAC with respect to other groups with*
> *adjacent or overlapping remits, including the SSAC, the RZERC, and the RSSAC Caucus.*

RSSAC's June 2018 publication, "A Proposed Governance Model for the DNS Root Server System", mentioned above, would require significant resources to implement. It is not clear if or how ICANN intends to implement this model. RSSAC currently has similar technical staff support from ICANN as SSAC does.

[20] https://www.icann.org/en/system/files/files/rssac-review-final-02jul18-en.pdfge2;zb3

Did the implementation have the intended effect? How was the assessment conducted?

It is not clear that this recommendation was implemented; however, it is unclear how to assess this recommendation given the wording.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

This recommendation is relevant, but requires reconceptualization as described above. A recommendation related to this topic included later in the report.

SSR1 Recommendation 24: ICANN must clearly define the charter, roles and responsibilities of the Chief Security Office Team.

What was done to implement the recommendation? Was the recommendation fully implemented?

As of 2018, there is no Chief Security Office; however, the OCTO (Office of the Chief Technical Officer) SSR team works on externally focused ICANN-related SSR issues, the CIO and team work on internally focused security issues, and the OCTO Research team looks towards future SSR risks and opportunities within ICANN's limited scope and remit. The OCTO-SSR team is led by John Crain. The OCTO-SSR team is described on this web page: https://www.icann.org/octo. This team has two additional people on it: Carlos Alvarez, "SSR Technical Engagement Sr. Manager Security" and Samaneh Tajalizadehkhoob, "Lead SSR specialist". The web page describes the mission of this team in high-level terms, and links to a page of "activities" at https://www.icann.org/octo-ssr. There is no language referring to "charter", "roles", or "responsibilities" of this team. The SSR2 team assumes that the activities listed on this page are what ICANN intends as the SSR-related roles and responsibilities of OCTO:

- Engage actively with security, operations, and public safety communities to gather and process intelligence data that indicate (imminent) threats to DNS or domain registration service operations (the "DNS ecosystem").
- Facilitate or participate with these same communities in threat preparedness activities to protect against or mitigate threats to DNS ecosystem.

- Perform studies or analyze data to better understand the health and well-being of the DNS ecosystem.
- Coordinate DNS vulnerability disclosure reporting (https://www.icann.org/vulnerability-disclosure.pdf).
- Lend subject matter expertise to build capability among ccTLD and public safety communities in subjects relevant to the DNS ecosystem, including DNSSEC, abuse or misuse of DNS infrastructures or operations.
- Assist in DNS ecosystem risk management activities.
- With ICANN's Global Stakeholder Engagements team, participate in a global, multi-stakeholder effort to improve cybersecurity and mitigate cybercrime.

[...]

The OCTO may also consider:

o Coordinate with appropriate agencies for the containment of cyber security incidents and Vulnerability remediation in their constituencies (eg: National CERTs, Government agencies etc.)

o Ensuring that Incidents are investigated and corrective action taken as identified through a comprehensive Root Cause Analysis (RCA)

Did the implementation have the intended effect? How was the assessment conducted?

To the extent that the articulation of roles and responsibilities were intended to enable community understanding and evaluation of ICANN's SSR activities, this description of roles and responsibilities is too vague to support such understanding. The SSR2 teams recommends that this list include a set of metrics by which one could evaluate progress on execution of these responsibilities, as well as periodic (at least annual) reports that report these metrics and provide details on SSR2-related accomplishments within ICANN.

A related problem is that OCTO does not seem to have produced much in terms of SSR analysis that is available to the public. The "Open Data Initiative", the DAAR reporting, and the Internet metrics project all seem to be projects with associated data that is internal to ICANN. It is not clear how useful any of this work has been thus far to the larger community that ICANN is intended to serve.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

This recommendation remains relevant, and we propose a new recommendation on this topic later in this report. We believe that ICANN must staff a full-time person that will coordinate across all SSR-related constituencies: Compliance, CCT, GDD.

SSR1 Recommendation 25: ICANN should put into place mechanisms for identifying both near and longer-term risks and strategic factors in its Risk Management Framework.

What was done to implement the recommendation? Was the recommendation fully implemented?

A Risk Management Framework has been accepted by the board in 2013, having received community input during ICANN50 and ICANN51. ICANN maintains an Enterprise Risk Management (ERM) Dashboard that lists risks to be monitored and addressed and follows an enterprise risk management framework. However, while a mechanism has been put in place, there is a lack of clarity in terms of how risk identification feeds into relevant SSR processes and policies.

Did the implementation have the intended effect? How was the assessment conducted?

While some material about near and long-term risk related to SSR is published, the mechanism for feeding this information into ICANN's Strategic Plans is not obvious.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

A regular review of near and long-term SSR-related risks remains relevant. It is necessary to consider the mechanisms to support such review, particularly how risk identification is performed and how findings would translate or feed into relevant policies and (risk management) frameworks.

SSR1 Recommendation 26: ICANN should prioritize the timely completion of a Risk Management Framework.

What was done to implement the recommendation? Was the recommendation fully implemented?

This recommendation correlates to R25. A Risk Management Framework has been accepted by the board in 2013, having received community input during ICANN50 and ICANN51. A more detailed response for this recommendation is addressed under the assessment for for R27.

Did the implementation have the intended effect? How was the assessment conducted?
Notably, given that the term "timely" does not a connate any specificity in what was intended or acceptable, it cannot be assessed if the intended effect was achieved.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

This recommendation is not relevant today. Rather than a timely completion, it is important for risk management practices and procedures to stay up to date, and for it to be reviewed regularly by the community, and findings and recommendations feed back into the Risk Management Framework. Furthermore, procedures that ensure measures are tracked and reviewed must be established as discussed in SSR1 Recommendation 25.

SSR1 Recommendation 27: ICANN's Risk Management Framework should be comprehensive within the scope of its SSR remit and limited missions.

What was done to implement the recommendation? Was the recommendation fully implemented?

The Review Team noted that there is a correlation between Recommendations 25, 26 and 27. During the review it was concluded that there is a Risk Management Framework is in place. However, in the absence of a definition of "comprehensive" by SSR1 or metrics for evaluation, it was very difficult to assess whether this recommendation has been implemented.

Did the implementation have the intended effect? How was the assessment conducted?

In doing the review, discussions surrounded, among other things, whether Recommendation 27 was implemented based on the references made by staff during various question and answer exchanges related to Recommendation 25. The Review team concluded however, that this Recommendation, while it correlates to Recommendations 25 and 26 is distinct, because it asks that the Framework should be "comprehensive." The Review Team was of the opinion that if R27 was implemented in line with what SSR1 Review Team intended, it would have addressed the concerns that R25 and R26 was probably seeking to address.

However, SSR1 gave no definition as to what elements of the framework would constitute "comprehensive" or how this should be evaluated. Further, during the review it was noted that this Recommendation would have implemented by ICANN staff that are no longer with ICANN. In this regard, institutional memory and a complete historical record of how they assessed "comprehensiveness" of the Risk Management Framework was not available.

It's worth noting that during the public review of the draft Risk Framework, comments were provided that suggested that some members of the community did not believe the framework to be comprehensive. Two examples of indicative comments[21] are below:

- "[Westlake's view that Availability, Consistency, or Integrity of the DNS is outside of the scope of the Risk Management Framework] is a very limited view of risk management focused only on whether the DNS is at risk – not whether everything in the Internet that relies on the DNS is." – Comment from Verisign
- "The ALAC deplores that at this point in time, the proposed Framework is far from being detailed at a more granular level" – Comment from ALAC

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

[21] https://www.icann.org/public-comments/dns-rmf-final-2013-08-23-en

This is still a relevant recommendation as from the Review, it was evident that publicly available information as to how risk management is addressed was found in piecemeal locations. As an example, staff indicated that the Board Risk Management Committee was made up of the ICANN Org executive team which provides oversight. Further, that there are function related risk liaisons who are staff members representing each function for implementing the risk framework, and all organization personnel who own the risks inherent in their activities, focuses on risk management issues. This demonstrates that the risk function for ICANN org has not been centralised and coordinated strategically. The Review Team also took note of the conclusion of the DNS Risk Framework Working Group and its Report[22] and the 2016 Identifier Systems Security, Stability and Resiliency Framework – for FY 15-16 [23] and recommends that these be taken into account as resource documents for the development of any RIsk Management Frameworks.

RECOMMENDATION

If one were to rephrase this Recommendation, the Review Team believes what was meant was '*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*'

SSR1 Recommendation 28: ICANN should continue to actively engage in threat detection and mitigation, and participate in efforts to distribute threat and incident information.

No Public data shows that ICANN engages in threat detection and mitigation. ICANN when feasible disseminates to responsible external third-parties vulnerabilities reported. However it is the responsibility of the third-party to act on the threat and incident information disseminated.

What was done to implement the recommendation? Was the recommendation fully implemented?

[22] https://www.icann.org/public-comments/dns-rmf-final-2013-08-23-en
[23] https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf

This is related to SSR1 **Recommendations 15 and 24.**

The OCTO-SSR team is led by John Crain, ICANN's Chief SSR Officer. The team strives to be trusted partners in collaborative efforts to ensure the security, stability, and resiliency of the Internet's global identifier systems. They educate and report using a variety of avenues to address these concerns.

1. Prevention through threat awareness and preparedness, collaboration and information sharing.
2. **Mitigation through information sharing and coordinated response**
3. Adoption of best practices through collaboration and capability building.
4. **Understanding through analysis of unique identifiers data, domain registration service data and other data associated with identifier systems.**
5. Security awareness through training activities.
6. Establishment of trustworthiness through transparency, communication and reliable execution.

The overall goal of OCTO-SSR programs is to ensure the security, stability and resiliency of the Internet's Identifier systems. To achieve this goal, ICANN will:

1. Engage actively with security, operations, and public safety communities to gather and process intelligence data that indicate (imminent) threats to DNS or domain registration service operations (the "DNS ecosystem").
2. Facilitate or participate with these same communities in threat preparedness activities to protect against or mitigate threats to DNS ecosystem.
3. Perform studies or analyze data to better understand the health and well-being of the DNS ecosystem.
4. **Coordinate DNS vulnerability disclosure reporting https://www.icann.org/vulnerability-disclosure.pdf**
5. Lend subject matter expertise to build capability among ccTLD and public safety communities in subjects relevant to the DNS ecosystem, including DNSSEC, abuse or misuse of DNS infrastructures or operations.
6. Assist in DNS ecosystem risk management activities.
7. With ICANN's Global Stakeholder Engagements team, participate in a global, multi-stakeholder effort to improve cybersecurity and mitigate cybercrime.

Did the implementation have the intended effect? How was the assessment conducted?

While we are confident that ICANN SSR team plays a coordinating role in distributing threat intelligence to involved parties and engages regularly with law enforcement, there is little or no public evidence that this has occurred. Furthermore, there is no public evidence that the ICANN organization conducts ongoing threat detection nor that anyone is tasked with this function. The ICANN community, however, has a number of groups (both open and closed) that actively conducts threat detection including SSAC, RSSAC, TLDOPS, ccNSO incident response WG, and PSWG. The ICANN SSR team coordinates with these groups.

Is the recommendation still relevant today? If so, what further work needed? If not, why not?

The recommendation is still relevant today.
A recommendation is in order.

NOTES:

Summary comments / Reappearing Issues: (make this a preamble to SSR1 Implementation, as well as recommendations, plus stats on implementation)

Accountability and Transparency

1. Lack of indicators, measurements, goalposts.
2. Lack of publicly available evidence, procedures.
3. Lack of community review and accountability.
4. Lack of overarching strategy, goals, or comprehensive policy.
5. Lack of clear definitions.
6. Lack of clarity (what is being done?)
7. Lack of integrated security management (e.g. policy, procedures, standards, baselines, guidelines, as in Sec Management)