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.

SSR Role and Remit was developed, and it received public comment and consensus: https://www.icann.org/resources/pages/ssr-role-remit-2015-01-19-en**. In addition, the SSR Framework is published and updated periodically. However, the definitions of Security and Stability contained in ICANN's agreements with contracted parties use a different definition for SSR. The SSR2-RT observes that ICANN's agreements with contracted parties (see section 7.3 of https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.docx) uses different definitions. Full implementation of this recommendation would require consistency across ICANN with the SSR Role and Remit document that has achieved consensus.**

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

- Public comment was taken on a draft statement between May-Sept 2012; it was subsequently revised in Oct 2012.
- The updated statement was published on ICANN's website and incorporated in the FY 14 SSR Framework and is part of SSR SOP in which SSR Framework and statement is periodically reviewed and updated as needed. This statement also has been incorporated into other ICANN documentation.
- SSR1 implementation report here (slides 1 - 3)
- FY 15-16 SSR Framework is here.
- SSR2-RT briefing slides on this recommendation here (slides 5 – 13).

Questions & Answers

1. Since the version developed in 2012, what changes have been made to the SSR remit and technical mission statement? Who has made those changes? How has the community been allowed to review and comment on those changes? When were the last changes made to this statement?
   - Answers to this question available here (published in in 2015): https://www.icann.org/resources/pages/ssr-role-remit-2015-01-19-en
2. How are the definitions of security, stability and resiliency consistently carried through into key documents, such as strategic plans and agreements with contracted parties?
   - Because of the variety of subjects that this question incorporates, it is difficult to address. Different departments work on different aspects of this question and don't always have visibility to the topics covered in the question. Because of this, ICANN ORG operates in a "Best Effort" model and reaches out to OCTO-SSR if any questions arise surrounding the use of the definitions. To date, ICANN ORG feels that it has stayed consistent with the usage of the definitions between the various types of documents.

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

No direct metrics were provided in Recommendations 1 to evaluate whether the implementation had its intended effect. There are indirect indications that the implementation of the recommendation did not have its intended effect.(DM)

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

This recommendation is extremely relevant and SSR2 has had significant discussions – both internally and publicly – on how to develop such a clear and consistent statement as well as how to get public feedback on that statement. It's worth noting that one of the differences between the draft SSR statement and the one finally published on the ICANN website is that the draft version has a section on "Responsibilities the lie outside ICANN's role in SSR." The version on the website also has a definition of Unique Identifier Health apparently added sometime between 2011 and 2014.

Further, the definitions of Security and Stability contained in ICANN's agreements with contracted parties are also different.[1]

ICANN's own status report indicates that the statement is periodically reviewed and updated as needed[2].

Further work may be needed to bring this to closure, especially because of the inconsistencies between different versions of the remit. The ToR for SSR2 would be a useful place to start.[DM]

---

[1] See for example clause 7.3 of the registry agreement updated 31 July 2017 https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.docx
[2] https://www.icann.org/en/system/files/files/ssr-review-implementation-30jun15-en.pdf

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

SSR Role and Remit was developed, and it received public comment and consensus: https://www.icann.org/resources/pages/ssr-role-remit-2015-01-19-en**. In addition, the SSR Framework is published and updated periodically: https://www.icann.org/en/system/files/files/ssr-plan-fy14-06mar13-en.pdf. However, it is unclear who is intended to conduct the recommended "review" -- the SSR review teams or someone else. Future SSR review teams can suggest changes, but of course, the changes cannot be adopted without community consensus. Note that the current definitions make it difficult for the SSR2-RT or anyone else to assess the implementation by ICANN.**

OBSERVATION: In recent years, updates to the SSR Framework have received community review, but this was not done for every update.

RECOMMENDATION: Updates to the SSR Framework should follow a published process that include community review. This process must to be aligned with the ICANN strategic Plan and the ICANN Operating Plan.

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

- The statement (and SSR Framework) informed ICANN's Strategic Plan for FY2016—2020, which reflects strategic SSR objectives, goals and key success factors (KSFs) for the next five years and was result of input and review by the ICANN community, Staff and Board. SSR elements are highlighted here.
- This, in turn, informed the new Five-Year Operating Plan, which also was developed with community input and includes SSR key performance indicators (KPIs), dependencies, five-year phasing, and portfolios. SSR elements are highlighted here.
- Periodic review of the SSR Framework, including the SSR role and remit statement, are part of the SSR SOP, and also will be reviewed by the next SSR RT in 2015.
- SSR1 implementation report here (slides 4 - 6)
- SSR2-RT briefing slides on this recommendation here (slides 4 – 29).

Questions & Answers

1. Recommendation 2 directs that the definition of ICANN's SSR remit and limited technical mission should be reviewed in order to maintain consensus and elicit feedback from the Community. Please provide details of reviews and community feedback that have occurred since 2013.
   - A summary of comments on the FY 2014 Framework was created in 2014 but was not posted to the ICANN org website due to an error. It will be posted in due course. The public comments can be found here: https://www.icann.org/public-comments/ssr-fy14-2013-03-06-en
   - Note that other SSR Framework documents that have been published since the FY14 document, which has been overtaken by events and is historical now.
2. As ICANN's SSR remit and limited technical mission statement has evolved, how has comment from the community been incorporated? For instance, is there a summary of the comments on the FY 2014

Framework? Where is this published?

- ICANN's SSR remit and limited technical mission are published in ICANN's SSR Framework and other documents. The SSR Frameworks are available at https://www.icann.org/ssr-document-archive. On this same page, OCTO has also posted other SSR updates, activity reporting and a recovery checklist. ICANN and its partner the Network Startup Resource Center have also published https://www.icann.org/news/blog/icann-and-nsrc-collaborate-on-training-events and see https://www.icann.org/news/blog/spreading-knowledge-in-2014-technical-training-with-nsrc. See also https://www.icann.org/news/blog/five-years-of-technical-training-in-apac-to-ensure-the-security-stability-and-resiliency-of-the-internet, and the Technology page on the ICANN website - https://www.icann.org/technology.
  SSR is a part of the Office of the CTO. OCTO publishes an activities brief (see the one from June 2018): https://www.icann.org/news/blog/office-of-the-cto-activities-brief-january-to-june-2018. https://www.icann.org/news/blog/the-three-pillars-of-icann-s-technical-engagement-strategy. The community is always able to provide input given ICANN's commitment to transparency but there is no official public comment process on the relationships.

2Did the implementation have the intended effect? How was the assessment conducted?

Yes, unclear whether the "review" meant that the SSR-RT was being tasked or someone else. SSR-RT can suggest changes, but they cannot be adopted without community consensus.

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

Ought to have community review whenever the SSR Framework is updated;
Ought each SSR-RT definition and implementation going forward.

Current definitions make it difficult for SSR-RT or anyone else to assess the implementation by ICANN.

there appear to have been no opportunities to comment specifically on the remit and mission statement in the five years since 2013. Given the the SSR activities and challenges ICANN faces, further work is needed in this case – specifically in regard to the recommendation's suggestion that there be regular reviews of that remit[DM]

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.

SSR Role and Remit was developed, and it received public comment and consensus: https://www.icann.org/resources/pages/ssr-role-remit-2015-01-19-en**. ICANN seems to be going the right things. Please continue to do so; however, not possible for SSR2-RT to review every document, so it is hard to determine whether the terms are used consistently throughout ICANN. However, the definitions of Security and Stability contained in ICANN's agreements with contracted parties use a different definition for SSR. The SSR2-RT observes that ICANN's agreements with contracted parties (see section 7.3 of https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.docx) uses different definitions. Note that the SSR2-RT did not find procedures that are used to ensure that the terms in the glossary are used in all material and communications.**

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

- Consistent terminology and descriptions related to ICANN's SSR role and remit have been publicized and are encouraged in all ICANN material.
- Key terms are added 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.
- Document of definitions across ICANN org available here (provided to RT in March 2017).
- SSR1 implementation report here (slides 7 - 9)

Questions & Answers

1. In what way has ICANN publicized consistent terminology and descriptions related to ICANN's SSR role and remit? Where are these published?
- Document of definitions is available here: https://community.icann.org/pages/viewpage.action?pageId=64074062&preview=/64074062/64076676/SSR%20Def_Steve%20Conte.pdf
2. What terms related to SSR have been added to the ICANN public glossary? When were they added?
- See here: https://www.icann.org/icann-acronyms-and-terms/en/G0301

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

The staff report on this recommendation has a link titled "Publicize consistent terminology and descriptions related to ICANN's SSR role and remit." The link does not resolve.[1]

There is a blog post on the ICANN blog from July 2013 that gives a list of ICANN's security terminology. However, this does not appear to be integrated into any other SSR-related documents. 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. The glossary has not been updated since February of 2014. There are no references to SSR, its remit or mission in the publicly available glossary.

It is very likely that the implementation did not have its intended effect.

---

[1] From the SSR Review Executive Summaries for Recommendations 1 – 28; "Fully Implemented as of April 2017"

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

Seems to be going the right things. Please continue to do so; however, not possible for SSR-RT to review every document, so it is hard to determine whether the terms are used consistently throughout ICANN. Did not find procedures that ensure that the terms in the glossary are used in all material and communications.

The recommendation seems to have a foundation in common sense, and merits SSR2's further consideration

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.

SSR2 RT Volunteers: Laurin

Detailed breakdown of ICANN's SSR Relationships is located at: https://www.icann.org/en/system/files/files/ssr-relationships-fy17-23jan17-en.pdf

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

- (Phase I) Many of ICANN's SSR relationships have been defined and publicized. As part of OCTO SSR Team SOP, this work will be updated periodically to keep pace with SSR activities. Memorandums of Understanding that indicate roles and responsibilities relevant to SSR have been signed with numerous entities; the list is posted here and will be updated as part of SOP, as needed.
- (Phase II) Extract and catalogue SSR-related elements of MOUs; Provide additional detail on formal relationships ICANN has with key organizations. This includes: 1) noting the "relationship," covering informal and formal arrangements; 2) documenting that some relationships are sensitive (not disclosed) and noting the industry best practices and conventions that are used to address this lack of disclosure.
- ICANN Security Awareness Resource Locator Developed - All stakeholders should learn how to protect themselves, their families, or their organizations against online threats. The resources on this page can help

consumers, business or IT professionals avoid online threats or harm and make informed choices regarding (personal) data disclosure or protection.

- The document tracking ICANN SSR related roles and responsibilities has been completed and posted at https://www.icann.org/en/system/files/files/ssr-relationships-fy17-23jan17-en.pdf
- SSR1 implementation report here (slides 10 - 12)
- SSR2- RT briefing on this recommendation here (slides 23 – 27).

Questions & Answers – **SOME ANSWERS OUTSTANDING – CLARIFICATION FROM RT REQUESTED**

1. What accounts for the inconsistencies between the different documents on the ICANN website that describe the nature of the SSR relationships it has within the ICANN community?

- CLARIFICATION SOUGHT: Could you please provide some concrete examples of discrepancies?

2. In what way are these documents fulfilling the requirement to provide a single focal point for understanding the interdependencies between organizations?

- MOUs are in place that have been incorporated as part of the agreements. We have several links in place for ICANN security resource locator development, and a document published in January of 2017, that identifies, in detail, all the relationships. This information can be found here:
- * ICANN's major agreements and related reports are published at: https://www.icann.org/en/about/agreements
- * Detailed breakdown of ICANN's SSR Relationships is located at: https://www.icann.org/en/system/files/files/ssr-relationships-fy17-23jan17-en.pdf
- * ICANN's Security Awareness Resource Locator page can be found at: https://www.icann.org/resources/pages/security-awareness-resource-2014-12-04-en

3. What opportunities have there been for community input into the nature/definition of ICANN's SSR relationships?

- This document is revisited and revised periodically with new versions being published as such. The community is always able to provide input given ICANN's commitment to transparency but there is no official public comment process on the relationships.

4. How is the document describing SSR relationships with partner organizations being updated?

- This document was prepared in accordance with recommendation 4. There is no established process in place for updating it.

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

No, the implementation did not have the intended effect.

Explanation:
The staff report on implementation indicates that the recommendation was fully implemented as of 31 December 2016, but references documents published after that. It seems that the key document for tracking ICANN SSR related roles and responsibilities is at:

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

The document appears to list 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. Furthermore, there are a lot of documents that provide "small pieces of evidence" rather than what the recommendation appears to request, and also what would be useful for the community. Many of the documents are described as: "document cannot be located online." Furthermore, in the main document, the SSR components of the relationships are often marked as "unknown."[1] Since the recommendation suggests that the document would be a "single focal point for understanding the interdependencies between organizations," it seems clear that the implementation did not have its intended effect.

This assessment is based on reviewing the documents provided by ICANN.org, and concluding that no single focus point with clear information is available.

---

[1] 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?

Yes - SSR relationships are extremely relevant for ICANN's mission and the maintenance of security and resilience.

Given questions and concerns related to nature of the ICANN's SSR relationships, further work is needed in this case. 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 the ICANN community. Further work is needed to update this document or to provide a new resource that meets the intent of the original recommendation. This could be a similar table that is kept up to date. It should indicate what relationships exist, how they work, 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.

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.

Detailed breakdown of ICANN's SSR Relationships is located at: https://www.icann.org/en/system/files/files/ssr-relationships-fy17-23jan17-en.pdf. The efficacy of relationship management was clearly not measurable.

Not included in Doodle poll. Russ led discussion on rec 5 during 27 September plenary, Laurin led discussion on rec 5 during 4 October plenary.

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

- (Phase I) Reporting on ICANN's progress toward SSR-related KSFs and KPIs involving SSR relationships is SOP, and can be found in ICANN's regular project management reporting, operating plans, SSR Framework, and SSR quarterly reports.
- (Phase II) Next SSR Framework/report on SSR activities will include information on how key relationships noted in Recommendation 4 are used to achieve SSR goals (as part of SOP).
- The document tracking ICANN SSR related roles and responsibilities has been completed and posted at https://www.icann.org/en/system/files/files/ssr-relationships-fy17-23jan17-en.pdf
- SSR1 implementation report here (slides 13 - 15)
- SSR2- RT briefing on this recommendation here (slides 23 – 27).

No questions & answers.

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

Laurin's comments: While evidence has been presented that ICANN has taken various steps to forge relationships, the team cannot assess if working relationships are effective (1), and furthermore, little evidence is visible regarding what these relationships entail and if they are effective (2). There is some evidence however, that ICANN succeeded in establishing relationships with relevant actors.

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

The ICANN OCTO 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. *Laurin's comments:* Where possible, insight into these relationships should be provided in an easily accessible format. Lastly, the recommendation specifically mentions maintenance, i.e. this is a constant, never-ending process.

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.

SSR2 RT Volunteers: Russ

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

The roles and responsibilities for SSAC and RSSAC are captured in https://www.icann.org/en/system/files/files/draft-rssac-ssac-roles-responsibilities-05mar15-en.pdf. However, this document is still marked as "DRAFT UNDER REVIEW." If consensus was achieved, a final document could not be located.

RECOMMENDATION:

> **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.**

****

Currently, 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.

RECOMMENDATION:

> **To facilitate the search after public comment is long over, ICANN should create a mail list 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.**

https://www.icann.org/en/system/files/files/draft-rssac-ssac-roles-responsibilities-05mar15-en.pdf captures the roles and responsibilites for SSAC and RSSAC. However, this document is still marked as "DRAFT UNDER REVIEW." If consensus was achieved, a final document could not be located.

- Roles and Responsibilities of SSAC are reflected in ICANN's Bylaws and defined in SSAC's Operating Procedures.
- Roles and Responsibilities for RSSAC are reflected in an updated charter contained in ICANN's Bylaws.
- SSAC and RSSAC have been asked to reflect their roles and responsibilities in a brief explanatory text for icann.org (linking to respective charters), and text as agreed to by the AC's chairs. April 2015
- SSR1 implementation report here (slides 17-18)

Questions & Answers

1. What is the status of the document currently available at: https://www.icann.org/en/system/files/files/draft-rssac-ssac-roles-responsibilities-05mar15-en.pdf?

- The role of the SSAC is published here: https://www.icann.org/resources/pages/ssac-role-2018-02-06-en. The role of the RSSAC is published here: https://www.icann.org/resources/pages/charter-2013-07-14-en

2. The recommendation requires that ICANN should seek consensus for this document across both groups. Please provide documentation that this occurred.

- The documentation to support consensus reached cannot be located, unfortunately due to passage of time since the recommendation was implemented.

3. What specific resourcing for RSSAC and SSAC appears in either the ICANN Operating Plan or the most recent budget?

- The support for RSSAC and SSAC is included in the ICANN Policy budget. Some of the service relies on

other team's services (web team, language services team, communication team) which are not easily quantifiable.

While draft operating plans and budgets since the SSR1 recommendations do address staff support for SSAC and RSSAC, there is no documentation on how decisions were reached regarding providing "appropriate resourcing." In fact, the currently adopted Operating Plan for ICANN makes no specific reference to resourcing for SSAC or RSSAC in any way.

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

No. The recommendation calls for a consensus document, and the documentation to related to the consensus process reached cannot be located.

It appears that work was started on this recommendation but not concluded and didn't address recent organizational reviews of SSAC and RSSAC. There is no specific document other than the March 2015 draft document, appear to be available.

Status of implementation: Not implemented.

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

Yes. This leads to two recommendations.

The consensus for the existing document cannot be confirmed.

RECOMMENDATION:

> 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.

Currently, 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 and their resolution for very long.

RECOMMENDATION:

> To facilitate the search after public comment is long over, ICANN should create a mail list 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.

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.

SSR2 RT Volunteers: Alain

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, which is necessary to fully implement this recommendation. Note that the SSR quarter reports page (https://www.icann.org/news/blog/identifier-systems-ssr-activities-reporting-en) has not been

updated since the summer of 2014.

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

- [Note: Recommendation was made before ICANN's current planning, budgeting and portfolio/project management and reporting processes were instituted].
- The Strategic and Operating Plans (see Recommendation 2) were informed by SSR Framework and reflect SSR priorities, objectives and activities. This is SOP for development of ICANN plans and budgets.
- SSR-related priorities, objectives and activities are reported on regularly as part of SOP, including in ICANN's regular portfolio management reporting and SSR quarterly reports.
- Revamped process for establishing updated SSR priorities and objectives. The ICANN Security, Stability and Resiliency department documented its Mission, Approach, Tasks in its August 2015 blog.
- The SSR Framework document archive is here.
- SSR1 implementation report here (slides 19 - 21)
- SSR2- RT briefing on this recommendation here (slides 4 – 29).

Questions & Answers

1. How are the objectives specific to the SSR Framework documented in either the Operating Plan or the Strategic Plan?

- The components of the SSR Framework are included in the ICANN strategic plan. SSR related KPI's in the strategic plan are related FY2016 –2020 Strategic Objective 2: Support a healthy, stable, and resilient unique identifier ecosystem:
- 2.1) Foster and coordinate a healthy, secure, stable, and resilient identifier ecosystem.
- 2.2) Proactively plan for changes in the use of unique identifiers and develop technology roadmaps to help guide ICANN activities.
- 2.3) Support the evolution of domain name marketplace to be robust, stable and trusted. Progress against these KPIs is available here: https://www.icann.org/accountability-indicators

2. Where are priorities for SSR activities and initiatives published?

- We have identified SSR related KPI's in the strategic plan. ICANN's strategic plan is here: https://www.icann.org/en/system/files/files/strategic-plan-2016-2020-10oct14-en.pdf. More details are available here: https://www.icann.org/resources/pages/strategic-engagement-2013-10-10-en

3. In what ways have pragmatic cost-benefit and risk analysis informed the choice of priorities (if any)?

- Over the last couple of years, risk & opportunity and financial assessments have been progressively entrenched to inform and drive prioritization. The FY18 Strategic Trend Outlook assessment was conducted with every functional team within org, the Board and community. The assessment results inform the annual operating plan update and budget and form the foundation for the next Five-Year Strategic Plan. Financial (cost/benefit) assessments have been a key focus within org, the Board and community in developing annual budgets and driving numerous cost-saving initiatives.

4. In addition to the ability to comment on draft ICANN budgets and plans, how is the community able to provide input into the objectives, initiatives and activities related to SSR at ICANN?

- As ICANN publishes its SSR frameworks, they are open to community review and comment. In light of the changes that took place during the IANA transition a new SSR Framework is currently in the making and will be published for review.

5. The SSR1 Report indicates that ICANN will "improve and publish a process for establishing updated SSR priorities and objectives." Where has this been published? Was there a mechanism for community review of the process (if so, please provide links)?

- A process has not been published. The SSR Frameworks incorporates ongoing feedback that is garnered from ongoing interactions with the community, including participation in technical and security forum (eg. APWG, MAAWG)

The most recent SSR Framework is from September of 2016.[1] The SSR Framework document does not list specific objectives for the SSR team – in addition, it does not prioritize them. Instead, it points to the ICANN Strategic Plan for this information.

Section 2.1 of the current strategic plan outlines ICANN's objectives (Key Success Factors) in the area of fostering and coordinating a healthy, secure, stable and resilient identifier ecosystem.

While all current projects for ICANN are listed at the ICANN Strategic Plan website,[2] there is no mechanism to determine when projects are related to SSR activities. The staff report also points to the SSR quarter reports page –

which has not been updated since the summer of 2014.

Status of implementation: Not implemented.

---

[1] https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf
[2] https://www.myicann.org/plan/projects

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. The level of detail envisioned in the recommendation doesn't seem to be provided in the public discussions of strategic planning at ICANN. There remains no obvious way for the ICANN community to provide 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?

In the interests of transparency and accountability the recommendation remains relevant today.

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.

SSR2 RT Volunteers: Laurin, Alain

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. The mechanisms envisioned by SSR1 have been replaced by other organizational and process tools.

RECOMMENDATION:

> **Going forward, the process used to develop the SOP should include more community involvement in setting the objectives and prioritization at more detailed level than is done today.**

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

- The Strategic and Operating Plans (see Recommendation 2) were informed by SSR Framework and reflect SSR priorities, objectives and activities. This is SOP for development of ICANN plans and budgets, in which SSR alignment is reviewed as annual plans/budgets are developed.
- Progress on SSR-related priorities, objectives and activities are reported on regularly as part of SOP, including in ICANN's regular portfolio management reporting and SSR quarterly reports.
- SSR1 implementation report here (slides 22 - 24)
- SSR2- RT briefing on this recommendation here (slides 4 – 29).

No questions & answers.

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

Laurin's comments: It is apparent that SSR is part of relevant reports and procedures. However, it is difficult to assess what priority SSR objectives take in reality. Reports do not give sufficient detail of implementation and execution of SSR activities.

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

As with 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 (lack of) 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. As with Recommendation 7, it would be useful to undertake more detailed and public objective setting with prioritization done via public, community input processes. Working out these processes would require new work at ICANN.

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.

SSR2 RT Volunteers: Laurin, Scott, Boban

No roadmap toward certification. Note that annual audit of several important functions is performed.

RECOMMENDATION:

> **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?

- ICANN's implementation of DNSSEC in the root has achieved SysTrust certification.
- ICANN launched its EFQM web page where the focus is on continuous improvement. The EFQM Excellence Model provides mechanisms for the holistic assessment of an organization. These assessments help improve the way ICANN works, so that it can deliver better results.
- SSR1 implementation report here (slides 25 - 27)
- SSR2- RT briefing on this recommendation here (slides 38 – 43).

Questions & Answers – **SOME ANSWERS OUTSTANDING**

1. SysTrust certification is referenced in the SSR1 Report as already in place. Please explain how it is claimed to be implementation of SSR1

- Certification options were assessed after the final SSR1 final report was published. Within the IANA Function's team, two different audits are completed on an annual basis. SOC3 Certification of Root Zone KSK System, and SOC2 Certification for our Registry Assignment and Maintenance Systems. These audits evaluate our service organization controls (SOCs) against the "Trust Services Principles and Criteria". This is a well-established framework that's certified by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants for assessing organization controls over security systems. More information is available here: https://www.iana.org/about/audits

2. Beside the certifications/audits done for processes in IANA, what certification activities have been assessed or implemented related to SSR?

- Answer outstanding.

3. For staff working on SSR-related objectives, is there a certification plan in place as part of career/staff development?

- Answer outstanding.

4. When was the EFQM model implemented within ICANN, and please provide details of how the SSR Framework and standard operating procedures have been evaluated and updated in the light of EFQM adoption to demonstrate process improvements over time.

- ICANN IANA functions have implemented the EFQM since 2009, and ICANN has also been implementing the EFQM model org-wide since FY15. The SSR Framework and standard operating procedures have been part of the process improvement assessment focus along with the model adoption. Has ICANN ever published a document that would include "a clear roadmap towards certification?" If so, where? Was there a mechanism by which community comment or engagement took place for such a document?

5. Has ICANN ever published a document that would include "a clear roadmap towards certification?" If so, where? Was there a mechanism by which community comment or engagement took place for such a

document?
- Answer outstanding

The staff report also indicates that ICANN has incorporated SSR-related certification into its EFQM program. However, there is no information available other than the SysTrust/SOC audits. While some DNS engineering staff were ITIL certified, this appears to have been done on a case-by-case basis.

It is not obvious how ICANN assessed certification options as a result of SSR1. It is also not obvious that ICANN ever published "a clear roadmap towards certification."

This recommendation was apparently not implemented.

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

Note: There is no documentation regarding the assessment of the certification options after the final SSR1 final report.

Annual SOC 2/3 Audits were carried out by a single company for several years in a row. Therefore, it is to be welcomed that a Request for Proposal: PTI Service Organization Control Audits (https://www.icann.org/news/announcement-2017-08-11-en) was published and awarded to a new company.

An examination of publicly available materials indicates that certification was pursued by individual staff and not on more general basis. It is also not clear if ICANN has ever published a document that would include a "Clear roadmap towards certification." ICANN seems to have focused on staff certification rather than organizational certification.

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

Yes. Laurin's comment: ICANN should establish a road map of what certification activities are being undertaken and what certifications it is aiming to achieve; ICANN should provide reasoning for their choice.

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.

SSR2 RT Volunteers: Denise, Scott

There is no doubt that ICANN's compliance function has stepped up considerably since 2011, when the SSR1 recommendation were made. ICANN produces monthly reports, providing much greater transparency 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 (https://features.icann.org/compliance/dashboard/0818/report).

Contractual compliance at the registry-level is managed through non-public processes, which are not measurable by this review, though we note the efficacy of that work. Analogous processes are clearly necessary at the registrar-level as well, and all of which need a publicly verifiable side-effect for this to be measured in the future. Any monitoring of a structured process needs to have a more detailed (and unambiguous) definition of that model first.

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

- Regular public reporting of compliance activities are part of SOP; detailed information is available here.
- Complaints migrated to icann.org and automated; bulk complaint tool launched; Pulse Survey implemented;

WHOIS inaccuracy qualities check launched; complaints submission processes & FAQs to address new 2013 RAA requirements completed; compliance auditing and outreached programs in place; new positions created to ensure fulfillment of goals and objectives in this area.

- SSR1 implementation report here (slides 28 - 30)
- SSR2- RT briefing on this recommendation here

Questions & Answers

1. Please provide a summary of the number of complaints and enforcement actions against registries and registrars taken by contractual compliance on the basis of SSR obligations in the past 5 years.

- ICANN has a dedicated public page for Contractual Compliance Reporting. This page provides three types of data to the ICANN Community. The first section, referred to as Metrics and Dashboards, provides monthly, quarterly and annual data. The second section, referred to as Contractual Compliance Metrics for a rolling 13-month period, provides ten different types of reports for a period of 13-month. The third section, referred to as Additional Contractual Compliance related data, provides links to the metrics and data specifically requested by different working groups
-
- The ICANN staff report gives the following as evidence that this recommendation has been implemented:
- · Reporting of compliance activities as part of standard operating procedures;
- · Launch a bulk complaint tool;
- · Implement Pulse survey;
- · Launch WHOIS inaccuracy qualities check;
- · Create complaints submission process and FAQs to address new 2013 RAA requirements;
- · Launch compliance auditing and outreach programs; and,
- · Create new positions to ensure fulfillment of goals and objectives in this area.
-
- There is no doubt that the resources for and reporting of compliance activities are more professionalized since the SSR1 review took place.
-
- Reporting of compliance activities is fairly comprehensive through the dashboard associated with this activity.[1] However, it is not clear the extent to which SSR issues are handled within the compliance process.
-
- The majority of the issues in the staff SSR1 implementation report highlight matters relating to WHOIS. The status of WHOIS is currently uncertain as a result of the coming into force of the General Data Protection Regulation, and ICANN's decision to redact personally identifying information from the public WHOIS. However, despite the redaction of public WHOIS, >80% of complaints against registrars in August 2018 related to WHOIS inaccuracy[2] an increase of more than 13% compared with the same period in 2017. Generally the volume of cases handled by compliance is increasing, and there is evidence of compliance activity directed at registries as well as registrars.
-
- WHOIS accuracy reporting has been underway since the 2012 WHOIS Review Team recommended the action[3]. The complaints submission process has been broken into three parts: a WHOIS Inaccuracy Complaint Form,[4] and a WHOIS Service Complaint Form.[5]
-
- The new registry agreement[6] contains specific obligations on contracted parties relating security and stability – including unauthorized disclosure, alteration, insertion or destruction of registry data, lack of compliance with RFCs. The registrar agreement (RAA 2013) contains fairly vague enforcement rights for ICANN in relation to registrars whose operation endangers Registrar Services, Registry Services or the DNS or the Internet[7]. Compliance enforcement reports for 2017 and 2016 contain little evidence of SSR enforcement actions. Data escrow formed the basis of one breach notice in 2017[8], and of 7% of complaints during 2016[1]. Otherwise, there is little information relating to SSR issues in the compliance reports.
-
- One of the factors mentioned in the SSR1 report is ICANN's goal to reduce the incidence and impact of registration abuse and malicious conduct. It is not clear to what extent this goal carries through into compliance actions or other initiatives aimed at reducing such conduct by registries or registrars.
-
- *Status of implementation: Partially implemented.*

-
-
- [1] https://www.icann.org/en/system/files/files/annual-2016-31jan17-en.pdf
-
-
-
- [1] https://features.icann.org/compliance/dashboard/0717/report
- [2] https://features.icann.org/compliance/dashboard/0818/report
- [3] https://whois.icann.org/en/whoisars
- [4] https://forms.icann.org/en/resources/compliance/complaints/whois/inaccuracy-form
- [5] https://forms.icann.org/en/resources/compliance/complaints/whois/service-form
- [6] https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.docx
- [7] https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en
- [8] https://www.icann.org/en/system/files/files/compliance-update-jun17-en.pdf
- r review teams.
- A summary of the number of complaints and enforcement actions against registries and registrars, including the number of complaints by complaint type can be found at https://features.icann.org/compliance/dashboard/report-list .
- As for enforcement, there are multiple reports to refer to:
- a) In the Metrics and Dashboards section, there are two reports to provide enforcement data; a report that presents data about the Formal Resolution Process broken out by enforcement reason (https://features.icann.org/compliance/dashboard/2018/q2/enforcement-complaint-type) and another that shows the data from a Compliance Approach & Process (https://features.icann.org/compliance/dashboard/2018/q2/complaints-approach-process-registrars) perspective for registrar and another for registry related complaints. Same reports can also be found in the Annual Report section.
- b) in the 13-month rolling section, there is a Formal Notices (https://features.icann.org/compliance/enforcement-notices) report that lists enforcement actions by a contracted party and the enforcement reasons for both registrars and registries

2. To what extent does ICANN measure the incidence and impact of registration abuse and/or malicious conduct by contracted parties?

- ICANN Contractual Compliance reports on the total number of registrar abuse report complaints received and processed. In late 2017, compliance reporting included the subject matter category in its monthly metrics; for example - the abuse complaint type now provides the subject of registrar related Domain Name System (DNS) abuse complaints such as spam, pharming, phishing, malware, and botnets in addition to counterfeiting, pharmaceutical, fraudulent and deceptive practices, trademark or copyright infringement, and registrar abuse contact.
- ICANN Contractual Compliance also proactively monitors compliance with the abuse-related obligations of the Registrar Accreditation Agreement and Registry Agreement through audits. At the closure of every audit round, ICANN published an audit report on the Reports & Blogs Page (https://www.icann.org/resources/compliance-reporting-performance). ICANN org is developing use of the information from the Domain Abuse Activity Reporting (DAAR) (https://www.icann.org/octo-ssr/daar) project for studying and reporting on domain name registration and security threat (domain abuse) behavior across registrars and registry operators.

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

There is no doubt that ICANN's compliance function has stepped up considerably since 2011, when the SSR1 recommendation were made. It has professionalized, and there is greater transparency about its work through the provision of monthly reports.

Whether this change was caused by implementation of SSR1 recommendation 10 is not at all clear. Many other factors, and changes to the DNS environment – including the launch of new gTLDs and the change in ICANN's financial fortunes that followed. There was also pressure from other actors within the community (eg the first WHOIS Review, and the ATRT first and second reports) advocating a strengthening of ICANN's compliance function. These drivers and events are more likely to have contributed to the strengthening of ICANN's compliance than the SSR1 report alone.

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

Yes, the recommendation 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 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.

SSR2 RT Volunteers: Norm, Matogoro

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. That said, some important things have been done to mitigate domain name abuse, including:

- **Under the GAC, 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.**
- **The DAAR system has created to reported on abuse trends across gTLDs and a number of abuse types.**
- **<<< Add recommendation from CCT review >>>**

<<< Does this include ebero, dns response times, etc >>>

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

- SSR1 implementation report here (slides 31-33)
- SSR2-RT briefing on this recommendation here (slides 4-5)

Questions & Answers - **SOME ANSWERS OUTSTANDING – CLARIFICATION FROM RT REQUESTED**

1. Is there any quantification or more detailed information on what the working relationship with the APWG has yielded?
   - 1) cross-community collaboration on APWG white papers, see https://apwg.org/resources/apwg-reports/whitepapers, including these topics:

- registrar best/recommended practices
- web vulnerabilities survey
- subdomain registration phishing practices
- whois data and phishing
- twice annual global phishing surveys

   - 2) cross-posting of SSAC documents for APWG community, again see https://apwg.org/resources/apwg-reports/whitepapers
   - 3) cross-fertilization of subject matter expertise

- incoming SSAC chairperson is originally from APWG community
- several SSAC members are originally from APWG community
- registry (e.g., Afilias, Org) and registrar (Blacknight, GoDaddy) staff have joined APWG

2. On the status and deliverables of Rec 11 it says that ICANN has implemented measures of success for the gTLDs, but we haven't seen how you've implemented measures of success for new gTLDs and IDNs. That's the first check mark, but what we've been provided with is a draft report of some ideas that you could do. How is that considered full implementation of this recommendation?
   - An independent consultant was hired to implement this recommendation. The consultant's report states, "The measures of success anticipated by the SSR RT in Recommendation 11 assume the existence of a community-based definition of "success" with corresponding metrics that could serve as the basis for measurement. These do not exist for the new gTLD program nor the IDN ccTLD Fast Track program. This report recommends that success criteria and measurements that have been developed for closely related

ICANN activities—particularly the Competition, Consumer Choice, and Consumer Trust Review Team (CCCT RT)—be considered responsive to Recommendation 11, and that the issue of appropriate SSR metrics specific to the new gTLD program and the IDN ccTLD Fast Track be revisited by the second Security, Stability & Resiliency of the DNS Review Team (SSR RT2)." The report can be found here: https://community.icann.org/display/SSR/Rec+%2311?preview=/56140534/64082817/SSR%20RT1%20Recommendation%2011%20Implementation%20Report-%20Final.pdf --Lyman Chapin

3. In looking at the dashboard for rec 11 and all the checkmarks including operational items, it's really unclear how staff defined and measured success related to SSR. It's hard to see how the basic spirit of this recommendation was implementation, especially with an idea paper from a consultant. But in terms of the last 5 years and what staff did to implement, it's unclear. Can you gather more information and provide more clarity and facts?

- As noted in the answers to previous questions, the report from the consultant indicated that the measures of the success need to be defined by the community since they do not exist. Due to unforeseen personal circumstances of the consultant, work on this implementation was delayed. The consultant was able to finish the work prior to April 2017, at which the report was posted.

4. The SSR1 Report refers to Specification 11 as applying to all new gTLD registries. Please provide reports on the number and type of security threats reported by registries under their Specification 11 obligations. Please give details of enforcement action(s) taken by ICANN's contractual compliance department in relation to Specification 11.

- Details regarding ICANN Contractual Compliance's enforcement of registry operator security threat reporting obligations under Specification 11 have previously been published in response to requests for similar information from the new gTLD Subsequent Procedures Policy Development Process Working Group at https://community.icann.org/download/attachments/58735937/New gTLD Subsequent Procedures Request for Data %28PIC%29.docx?version=1&modificationDate=1502819042000&api=v2.
- To date, ICANN has issued two breach notices related to Specification 11. Both were on the basis of noncompliance with Section 3(c), regarding transparent operation of the subject top-level domain. Details regarding these notices are published at https://www.icann.org/uploads/compliance_notice/attachment/911/serad-to-westerdal-16mar17.pdf and https://www.icann.org/uploads/compliance_notice/attachment/1049/serad-to-allain-11jul18.pdf.
- No enforcement actions have been issued to date on the basis of Specification 11 3(b), regarding security threat reporting. Additionally, ICANN Contractual Compliance has recently conducted a registry audit which focused on registry operator compliance with Specification 11 security threat reporting obligations. An audit report regarding this audit round is estimated to be published by the end of October 2018 at the audit reports page, which can be linked to from https://www.icann.org/resources/pages/audits-2012-02-25-en.

5. In a commercialized world of DNS service provision where data is considered to be a corporate asset, do you feel that either ICANN or the community at large have access to meaningful metrics? I cite the barriers that exist on information on root servers. Is this a barrier to the entire objective, that access to data appears to be challenging?

- Geoff Huston (asker) clarified that he feels this is a question for the review team to answer, not ICANN org.

6. Do you think it is ICANN staff's responsibility to gather, analyze and publish this data or do you feel that it's ICANN's responsibility to facilitate others to do that?

- ICANN as an organization looks to community to define what success is especially in a program like that like the New gTLD Program and the IDN Fast Track program from the ccNSO. I don't believe ICANN imposes measures of success on those groups. And I think it's a community effort in which we look for guidance from the community on what those measures are. And then depending on what the result is, it would determine whether or not ICANN is the implementer of those measures of success or the shepherd of those measures. One of the challenges that we faced specifically around this recommendation and around those programs was that we didn't have any community definition of success or those measures, so we couldn't have any baseline in which to conduct measurements off those.

7. Please provide details of the measures of success relating to new gTLDs and IDNs that expressly address SSR related program objectives. The link in the SSR1 Report (https://community.icann.org/display/SSR/Rec+%2311) did not resolve.

- The implementation report for recommendation 11 can be found here: https://community.icann.org/display/SSR/Rec+%2311?preview=/56140534/64082817/SSR%20RT1%20Recommendation%2011%20Implementation%20Report-%20Final.pdf

8. Please provide a copy of the report referred to in bullet point 9 of recommendation 11 implementation in the Final Implementation Report. Given that the SSR objectives referred to in the report remain 'to be defined' please provide an explanation as to why this recommendation is said to be complete.

- The link to the report is here: https://community.icann.org/display/SSR/Rec+%2311?preview=/56140534/64082817/SSR RT1 Recommendation 11 Implementation Report- Final.pdf. The work was deferred to the SSR2 Review Team

as stated in the report. As such, this recommendation was marked as complete because the work could not progress any further without the SSR2 Review Team taking this on.

9. Are there any updates on the status of Coordinated Vulnerability Disclosure Reporting since 2013?

- This link contains the latest information that has been published.: https://www.icann.org/news/blog/icann-coordinated-disclosure-guidelines

10. What was happening in the 5 years between when the recommendation was approved by the Board and when a draft consultant report was posted in April 2017?

- We cannot speak for the first few years after the recommendation was approved by the Board because the staff working on the recommendation are no longer at ICANN org. At the point from when we do have a record of when the work was started, a consultant with the appropriate expertise was brought on board to implement the recommendation. Due to unforeseen personal circumstances of the consultant, work on this implementation was delayed. The consultant was able to finish the work prior to April 2017, at which the report was posted.

11. Considering staff and community feedback, how effective is the EPSRP mechanism (the second security and stability review in the IDN ccTLD Fast Track) in detecting and preventing stability and security issues other than consumer confusion?

- Answer outstanding

12. How many new gTLD applications were failed (or placed in contention or required to take additional steps) on the basis of the (i) the security and stability review or (ii) the string similarity review.

- Answer outstanding

13. In relation to the IDN ccTLD Fast Track, please give details of any strings that have failed those security and stability checks for security and stability related reasons rather than for consumer confusion – a CCT Review issue.

- Answer outstanding.

14. Noting IAG-CCT produced 70 metrics of which a single one (1.13) related to security issues; please provide details of the information gathered according to that metric. The web page of metrics and measures does not include information relating to 1.13.

- Section 3.20 of the 2013 RAA requires registrars to give ICANN notice within seven days of any unauthorized access to or disclosure of registrant account information or registration data (among other things). The notice shall include a detailed description of the type of unauthorized access, how it occured, the number of registrants affected and any action taken by the registrar in response. Although registrars are encouraged to provide ICANN Contractual Compliance with such notice (see https://www.icann.org/resources/pages/bankruptcy-breaches-2014-01-29-en) to avoid a potential compliance escalation, registrar may also provide such notification to ICANN org via other means.
  In January 2015, ICANN Contractual Compliance collected data for the Competition, Consumer Trust and Consumer Choice Review team (metric 1.13) regarding the number of security breaches reported to it by registrars under Section 3.20 of the 2013 Registrar Accreditation Agreement (RAA) through the end of 2014. In consideration of the above request, ICANN Contractual Compliance has updated that data through the end of 2017:
  2012: 0
  2013: 2
  2014: 1
  2015: 1
  2016: 0
  2017: 0
  Additionally, as of this response, ICANN has received one registrar security breach notification in 2018.

15. Please provide details of how SSR objectives are explicitly referenced in ICANN's standard operating procedures, Service Level Agreements and monitoring, emergency back- end registry operators and data escrow, Trademark Clearinghouse, root zone scaling management, DNSSEC-related activities, and Compliance Dept. activities.

- Answer outstanding.

16. The SSR1 review team called out a number of activities that were operational and within staff's purview and contained in the SSR framework and called for implementation of measurements and metrics. Was that work done and is it captured anywhere? To clarify, as part of the SSR1 report related to rec 11, the SSR1 review team noted ICANN administration of the new gTLD Program, IDN program, significant SSR related issues that are in the framework. They called for more specific goals, measurements and impact assessment. Was that work done and is it captured somewhere else?

- Answer outstanding.

17. To what extent was the commissioning of the CDAR report, the Root Stability Study Workshop and the new gTLD program security and stability impact triggered by the SSR1 recommendation, and why is the SSR1 Report not referenced in the published materials relating to those initiatives?

- Answer outstanding.

18. What measurements exist, and are used, for the effectiveness of mechanisms to mitigate domain name abuse, as required in recommendation 11?

- Answer outstanding.

19. Which sections of the revised new gTLD registry agreement does OCTO staff feel advance SSR best practices and objectives?

- The revised new gTLD registry agreement contains SSR elements throughout. Many elements of the contract are there to advance SSR best practices and objectives. Highlights include but are not limited Article 2.3 (Data Escrow), Article 2.7 (Registry Interoperability and Continuity), Article 2.13 (Emergency Transition), Article 2.16 (Registry Performance Specifications) and 2.17 (Additional Public Interest Commitments) and associated Specifications. Article 3 sets out elements that advance SSR through clarifying expectations about such things as timely changes to the root zone.

20. Within the area of recommendation 11 & 12 activities for which ICANN can be a facilitator or convener – is there more information on the steps that ICANN took over the past five years to facilitate activities that involve other entities that had primary ownership or responsibility on related activities?

- Answer outstanding. CLARIFICATION SOUGHT: We're not clear on what the question is asking.

21. From the document here: https://community.icann.org/download/attachments/58735937/New%20gTLD%20Subsequent%20Procedures%20Request%20for%20Data%20%28PIC%29.docx?version=1&modificationDate=1502819042000&api=v2 "ICANN is in the process of updating the current complaint and reporting systems to enable enhanced granularity in reporting on the complaint types, including by legacy and new gTLDs. As a result of that, ICANN plans to publish this information on ICANN.org, along with the information provided to this Working Group in May 2017 following its request for information regarding compliance matters related to vertical integration. Target completion of this effort is July 2017 timeframe." Was this ever done?

- Yes. Work completed in July 2017 and publication began in August 2017. It can be found at this link - https://features.icann.org/compliance; we also published blogs in 2017 and 2018 about Enhancing Transparency in Contractual Compliance Reporting at this link - https://www.icann.org/resources/compliance-reporting-performance
  Specifically, additional granularity can be found in the Monthly dashboard; new Quarterly and Annual reports also. Please refer the Metrics and Dashboard section on that page. Regarding Vertical Integration questions – please refer to Additional Contractual Compliance section on same page.
-

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, so it is somewhat surprising that no metrics for evaluating compliance to these obligations appear to exist.

Security and stability reviews under the IDN ccTLD Fast Track process have focused entirely on the issue of visual confusability of strings. 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.

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[1].

The staff paper mentioned that a report was developed 'to inventory numerous activities within multiple ICANN departments that have the potential to support to-be-defined SSR objectives for the new gTLD and IDN fast track programs.' No link is given to the report, and it appears that despite the new gTLD and IDN fast track programs having been in existence (or advance planning) since the SSR1 report, it appears that SSR objectives required by the SSR1 recommendation remain 'to be defined'.

---

[1] https://www.icann.org/en/system/files/files/vulnerability-disclosure-05aug13-en.pdf

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

No. Recommendation 11 was aimed at embedding SSR considerations into expansion of the DNS space (either through the new gTLD program or the ccTLD IDN Fast Track) through appropriate metrics and risk mitigation measures.

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 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.

SSR2 RT Volunteers: Denise

*(Will add text as suggested by Naveed regarding the fact that while our team identified activities that are relevant to SSR-related best practices, there did not undertake a concerted, documented effort to work with the community to identify and implement SSR-related best practices)

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 this recommendation. 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 Internet.

RECOMMENDATION:

> **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 establish best practices for the improvement of SSR.**

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

Questions & Answers - **SOME ANSWERS OUTSTANDING**

1. Is there a central, up-to-date resource to see how the ISSSR team, and other professionals in the SSR field, have worked with SOs and ACs to identify additional, targeted best-practices for their constituents? Are there pointers to or records of those engagements?

- Interactions with SOs and ACs are documented through the regular ICANN processes. SSR interactions 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 these are not documented by OCTO SSR. More information about the ccNSO TLD-OPS can be found here: https://ccnso.icann.org/en/resources/tld-ops-secure-communication.htm

2. Has there been a Global DNS Stability, Security and Resiliency Symposium since 2014?

- No there has not. There have been other symposia such as IDS.

3. What has changed after the implementation of Rec#12 as compared with the past?

- Recommendation 12 has 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.

ICANN's OCTO Team works closely with Global Stakeholder Engagement Team in order to help facilitate and clarify some of the needs of the GSE regional strategies as they're being built. More visibility to the strategies in draft form helps OCTO to make sure we have the right resources and budget in order to support the activities that ICANN's regional VPs want to facilitate within the region. Earlier visibility to the regional strategies gives us a chance to be more responsive and proactive on the ground in supporting the GSE Team in the regions.

Although OCTO SSR is completely request-driven, we used to be completely ad hoc request-driven, which means that a request would come in, we would go and satisfy that. This was cost-prohibitive and inefficient. Now we are more deliberate in our actions, especially traveling and being physically in the region. We work with the GSEs prior to any travel to try to utilize team members time with meetings and presentations that are relevant during their travel to maximize efficiency. So, we set up meetings with key delegates in the region or we might be doing a training on DNSSEC but at the same time, while we're out in that region, we might also meet with local law enforcement or the regional Interpol, for example.

4. In what way have the recommendations contained in the paper, "Identifier System Attack Mitigation Methodology," been integrated into contracts, agreements and MoUs as envisioned by SSR1 recommendation 12?

- The Identifier System Attack Mitigation Methodology paper is a non-exhaustive list of attacks against the Identifier System that has been put forth for consideration within ICANN and by Identifier System security experts throughout the community. Although there have been some agreements/renewals/specifications/MOUs since February 2017, nothing specifically from this paper has been included in the contracts.

5. Is the only place where ICANN has documented work on recommendations for web application protection and development of resources for security awareness in the report from the 4th Global DNS Stability, Security and Resiliency Symposium?

- Yes

6. 'Addressing SSR practices in MOUs' links to a page that holds all of the MOUs. Can you provide some quantification of SSR-related practices in MOUs and more information on which ones contain SSR-related practices, which practices they contain, and how all that's tracked or the implementation is assessed?

- Answer outstanding.

7. What are some examples of significant MoUs with international entities that have SSR-practices embedded within them?

- Answer outstanding.

8. With regards to establishing best practices and integrating these into agreements to which ICANN enters: The SSR1 report is linked to a paper that raises a whole host of issues and addresses proposed activities but it's unclear how that then relates to integrating those into agreements into which ICANN has entered over the past 5 years. Can you provide more specific information on how best practices are reflected in agreements that ICANN has entered into?

- Answer outstanding.

The report linked to is entitled "Identifier System Attack Mitigation Methodology" and dated February 2017[1]. The paper sets out a number of 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.

No evidence is provided 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, Developing and Improving African Expertise; and project 4, encouraging resiliency of local DNS infrastructure. While these appear in the Regional Engagement Strategy documents – and while the ISSSR team reports on meetings in these regions – it is not evident that the outreach being done by the ISSSR team is a coordinated response to strategic regional engagement documents

The staff report indicated 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.

As we have seen previously, Specification 11 of the new Registry Agreement contains substantial SSR obligations on registries. The staff report for recommendation 12 indicates that the new RA is an example of a deliverable that meets the requirements of recommendation 12. However, the obligations in this RA have been part of the standard new gTLD registry agreement since applications opened in 2012. In the time between 2012 and 2017, ICANN has apparently not used these provisions as a baseline for assessing how effective they are in meeting the goals of recommendation 12.

Status of implementation: Partially implemented.

---

[1] https://www.icann.org/en/system/files/files/identifier-system-attack-mitigation-methodology-13feb17-en.pdf

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

No implemented so effect not assessed.. The assessment was conducted by reviewing the briefing materials provided by staff, interviews with staff, and following links to supporting materials.

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

SSR2 RT Volunteers: Naveed

We have no evidence to suggest whether this was done or not.

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

- As part of SOP, ICANN staff contacts all SOs and ACs (via chairs) to encourage identification and publication of a best practices repository page that is responsive to their constituencies. The ccNSO currently publishes SSR-related best practices information for their members.
- ICANN staff engages in a variety of ongoing activities to encourage global use of SSR best practices, as part of SOP (see Recommendation 12).
- Activity in this area is ongoing as part of SOP and ICANN builds on its activities annually. In 2015, for example, ICANN anticipates the creation of a set of resources of best practices for securing collaborative community assets. These resources will help SOs and ACs make informed decisions regarding identity management and data protection. From these, SOs and ACs could set requirements for how community assets should be made secure, stable and resilient.
- SSR1 implementation report here (slides 37-39)

Questions & Answers

1. In what way are the resources on the ICANN Security Awareness Resource Locator supposed to help Supporting Organizations secure collaborative community assets?

- In order to help the community learn how to protect themselves against online threats, the ICANN Security Awareness Resource Locator was published. An example of how some of the content of this page was utilized can be found here: https://ccnso.icann.org/en/resources/cybercrime-resources.htm

2. Have any recent steps been taken to encourage SOs and ACs to produce and publish best practices repositories for SSR-related information? Is the 2012 information on the ccTLD website the most recent example of SSR-related information published by a Supporting Organization?

- Staff is 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. As such, 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.

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

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

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

SSR2 RT Volunteers: Eric

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. The SSR communities are not a stationary set and always evolving. It is critical for ICANN to stay in-step and plugged in with them. Having some visible machinery and measures in place that tracks the SSR communities and assesses their relevance to ICANN's SSR is an important ongoing activity that does not appear to be addressed.

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

- Outreach activities have been expanded and are reviewed annually as part of SOP (Standard Operating Procedure). The Security team provides both a service function to ICANN's Global Stakeholder Engagement team as subject matter experts, and a community function in outreach and engagement in SSR matters. A new Engagement Interface allows the community to see upcoming SSR and related outreach and engagement activities. This is an on-going obligation.

- SSR1 implementation report here (slides 40-42)
- SSR2-RT briefing on this recommendation here (slides 28-32)

Questions & Answers

1. In the ICANN Engagement Interface, are all the SSR-Related outreach activities recorded or listed?
   - Yes, Global Stakeholder Engagement does have a tool where we capture our engagement events, called ICANN CRM. We are working to streamline the ICANN CRM in FY19-FY20 so that it captures all of the SSR-related outreach activities. Starting with FY19, Global Stakeholder Engagement will be reporting on its work across five areas:

• Capacity Development (which includes technical training and related engagement in the regions to support stakeholders become active participants in ICANN's technical and policy work)
• GSE Administration (This project covers administrative functions for the Global Stakeholder Engagement team, such as management of department budget, personnel, visas, allocation of resources.)
• Engagement Measurement and Planning (Project coordinates GSE Engagement, Measurement & Planning function, maintaining team goals and measurement of engagement. Management of GSE processes and procedures, inputs into ICANN CRM.)
• Cross-Organizational Collaboration (This project covers cross-regional and functional coordination activities for GSE with other ICANN Org departments (contributions to ICANN Strategic & Operational Planning, Community Engagement & Policy, event tracking, GDD-GSE engagement collaboration, support for Policy implementation, inputs to Enterprise Risk Management, inter-departmental collaboration). Travel and logistics for participation in ICANN Org workshops, regional meetings).
• Facilitation of Regional Participation in ICANN (This project covers Global Stakeholder Engagement work for enhancing cooperation and partnerships regionally to lower barriers to participation among stakeholder groups, and increase regional engagement within ICANN in its technical & policy work. This project includes the regional engagement plans and strategies, facilitation of regional events such as ICANN Readouts, regional DNS Forums, regional event sponsorships, contributions and collaborations).

2. When is the Annual Report for FY 2016-2017 going to be published as a community resource?
   - The draft SSR Framework is expected to be published for Public Comment within 2018.

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?
Yes. 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.

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

SSR2 RT Volunteers: Ram Krishna, Scott, Noorul

<<< **Scott to provide text by mid'ish-October.** >>>

In August of 2013, ICANN published a "Coordinated Vulnerability Disclosure Reporting at ICANN" document[1]. The document describe the reporting methodology for vulnerabilities identified by third-parties. Specifically, the document says: "The methodology ICANN describes here for vulnerability reporting also applies to reporting threats to the security, stability, or resiliency of Internet identifier systems."

Since 2013, none of the IS-SSR reports contain any statistics, metrics or lists related to disclosure reporting. It is impossible to tell from published materials if the vulnerability disclosure reporting methodology has ever been invoked. In addition, no data, even in anonymized form, is available about ICANN as a vulnerability coordinator, its work in emergency coordination and SSR-related crisis management.

The staff report on SSR1 also indicates that "staff collaborates with operators and trusted security community entities on DNS security threats and mitigation techniques." Necessarily, much of this work needs to be done in private. However, as with the coordinated vulnerability disclosure reporting, there is no public record of this activity, even in anonymized forms.

As a result, it is impossible to tell – from available, public information – whether or not this recommendation has been

implemented.

---

[1] See https://www.icann.org/en/system/files/files/vulnerability-disclosure-05aug13-en.pdf

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

- ICANN published a Coordinated Vulnerability Disclosure document in 2013. While the framework and SOP is in place, staff notes that because facilitation of responsible disclosure is an on-going obligation the work in this area is ongoing.
- Staff collaborates with operators and trusted security community entities on DNS security threats and mitigation techniques. This is related to Recommendation 28.
- The Identifier System Attack Mitigation Methodology report can be found at: https://www.icann.org/en/system/files/files/identifier-system-attack-mitigation-methodology-13feb17-en.pdf
- SSR1 implementation report here (slides 43-45)
- SSR2-RT briefing on this recommendation here (slides 33-35)

Questions & Answers

1. Are there any metrics or statistics available for ICANN's engagement with operators and trusted community entities on DNS security threats and mitigation techniques?
- Such events are normally kept confidential unless the effected parties wish to discuss them openly. We do not have statistics.
2. Is there any record of the methodology in the Coordinated Vulnerability Disclosure Document ever being invoked since 2013?
- The most noted was the JASBUG. After that, the only issue that invoked a process was the recent Adobe issue. ICANN has notified DNS providers of bugs when/if we find them but this does not invoke the process.
3. Are there any statistics available for the processes identified in the Coordinated Vulnerability Disclosure Document?
- There are no statistics available for the processes as the process itself has been invoked frequently enough to warrant the investment of resources to track specific details.

it is impossible to tell – from available, public information – whether or not this recommendation has been implemented.

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

If the intent of Recommendation 15 was to have ICANN develop and support a vulnerability disclosure process, the Recommendation was a success. There are no, public, statistics on how often such a process has been invoked. SSR2 might consider whether or not there any metrics or statistics available for ICANN's engagement with operators and trusted community entities on DNS security threats and mitigation techniques.

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

The motivations behind this Recommendation remain relevant today. SSR2 may choose to consider whether metrics for this activity are appropriate in the interests of transparency.

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.

SSR2 RT Volunteers: Eric

There is ongoing outreach by ICANN to related communities, which accomplishes the "participation" objective. However, outreach to additional SSR communities is encouraged. There is no evidence that current outreach activities have resulted in expanded Community participation. There is no evidence of a process for "systematic[ally]" incorporated from other ecosystem participants.

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

- Outreach activities and processes solicit input on the SSR Framework have been expanded and are part of ICANN's SSR SOP; activities are ongoing and are reviewed annually. For example: the Security team's ongoing work with security communities including the Anti Phishing Working (APWG), the Messaging, Malware and the Mobile Anti-Abuse Working Group (MAAWG) has resulted in participation by members of those communities in SSAC; through engagement with the International Criminal Law Network (ICLN) and Commonwealth Cybercrime Initiative (CCI), the Security team emphasizes the value of multistakeholder approaches to cybersecurity issues.
- Several Regional Engagement Strategies include SSR best practices and SSR topics are addressed by ICANN across all global regions. This is related to Recommendations 4, 5 and 14.
- At the request of stakeholders, the OCTO SSR team supports a variety of capability-building initiatives, such as DNSSEC training, ccTLD attack and contingency response training, law enforcement training, outreach at Network Operator Group meetings such as Caribbean Network Operators Group (CaribNOG), Middle East Network Operators Group (MENOG), among others.
- SSR1 implementation report here (slides 46-48)
- SSR2-RT briefing on this recommendation here (slides 38-41)

Questions & Answers

1. Are the documents that used to be called Frameworks, now to be SSR Annual Reports? If so, what is the community engagement mechanism being used for the Annual Reports?

- No. They are called Frameworks but had been named incorrectly on the SSR document archive. This page https://www.icann.org/ssr-document-archive has been updated with this correction.

2. What public engagement was done for the creation of the Frameworks and Annual Reports?

- Outreach activities and processes solicit input on the SSR Framework have been expanded and are part of ICANN's SSR SOP; activities are ongoing and are reviewed annually. For example: the Security team's ongoing work with security communities including the Anti Phishing Working (APWG), the Messaging, Malware and the Mobile Anti-Abuse Working Group (MAAWG) has resulted in participation by members of those communities in SSAC; through engagement with the International Criminal Law Network (ICLN) and Commonwealth Cybercrime Initiative (CCI), the Security team emphasizes the value of multistakeholder approaches to cybersecurity issues. Information is available here: https://www.icann.org/news/blog/identifier-systems-ssr-activities-reporting-en

3. Is there a record showing how Community participation and input into the SSR Framework was incorporated?

- Whenever a new framework is drafted it goes out for comment, which has it's own ICANN processes.

4. The implementation report specifically mentions capability building initiatives that would affect greater engagement in the development of the SSR Frameworks or Annual Reports. What initiatives have taken place? Who has participated? How have they expanded participation and input into the SSR Framework development process?

- Outreach by the SSR team is documented in various forms, for example through the engagement portal, SSR Activity reports and statistically through ICANN KPIs. All engagements are used as constant input into the development of the SSR frameworks and activities. SSR staff are currently writing a revision of the SSR Framework that will take into account the changes that occurred in the transition. That is taking longer than originally planned due to the need for a new approach.

Finally, recommendation 16 is clearly about expanding community participation and engagement in the SSR development process. It 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?
In part. 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

As with the two recommendations on integration of SSR related activities with the strategic plan, 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?

Yes, very much. The SSR space is very non-stationary and needs to both be kept up with, and interacted with.

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.

SSR2 RT Volunteers: Scott

This recommendation calls for more structured internal process in the development of SSR objectives and priorities, but public material does not provide evidence that this has happened.

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 get regular public consultation. Recommendation 17 asks 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. As we have seen, 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 activates and initiatives relate to specific strategic goals, objectives and priorities in the SSR Framework is present, it isn't obvious to a consumer of information on the ICANN website. However, the section of the most recent Annual Report which identifies annual initiatives does attempt to relate them to ICANN's Strategic Plan.

- See Recommendation 2 for information on how activities and initiatives relate to SSR priorities, objectives and goals and are integrated into ICANN's planning, budgeting and project reporting efforts.
- SSR1 implementation report here (slides 49-51)
- SSR2-RT briefing on this recommendation here (slides 4-29)

Questions & Answers

1. What is an example of a more structured internal process for showing how activities and initiatives relate to specific strategic goals, objectives and priorities in the SSR Framework? Has this been incorporated into the internal "At Task" system or other internal management systems?

- All goals are incorporated into our internal systems that track activities to the strategic priorities. At-task is one of these systems.

2. Are there any metrics or statistics available for ICANN's engagement with operators and trusted community entities on DNS security threats and mitigation techniques?

- Such events are normally kept confidential unless the effected parties wish to discuss them openly. I do not believe we have statistics.

3. Are there any statistics available for the processes identified in the Coordinated Vulnerability Disclosure Document?

- There are no statistics available for the processes as the process itself has been invoked frequently enough to

warrant the investment of resources to track specific details.

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

As seen with other Recommendations that attempt to align and integrate ICANN's SSR activities with the overall Strategic Plan, implementation of Recommendation 17 falls well short of providing a structured internal process.

Status of implementation: Impossible to tell 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 is still relevant. Like other Recommendations where the target was greater community participation in the development of objectives and priorities, Recommendation 17 is worth reconsideration by SSR2 with better metrics for evaluating the success of the implementation of the Recommendation.

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.

SSR2 RT Volunteers: Scott

This has been completed annually except for FY15-16. Not sure on the status of FY18, since it is not on the web site yet.

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

- Implemented as part of the FY 13 & FY 14 SSR Frameworks and will be repeated annually.
- The previous status of SSR RT implementation was published in Appendix C of the ATRT2 Report
- Elements of the SSR Framework are reflected in the Strategic and Operating Plans and budgets, with the status/progress being reviewed and reported annually for public input prior to the issuance of the following-year's Ops Plan and budget. Information is posted here.
- SSR objectives and goals are integrated into ICANN's Organizational (structural) reviews, as appropriate; these are scheduled every five years.
- SSR1 implementation report here (slides 52-54)
- SSR2-RT briefing on this recommendation here (slides 14-16)

No questions & answers.

Recommendation 18 suggests a recursive approach towards operational review: 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?

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?

This Recommendation should be reconsidered and reissued in a form that can be effectively assessed in the future.

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.

SSR2 RT Volunteers: Naveed

*** Revisit when the question is answered ***

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.

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

- The publication of the annual SSR Framework tracks progress against the activities committed to in the previous year's Framework. This tracking mechanism, along with ICANN's regular project management reporting, and operating plans and budgets, provide more details on SSR (see Recommendation 2 for more information) and are all part of ICANN's SOP.
- SSR1 implementation report here (slides 55-57)
- SSR2-RT briefing on this recommendation here (slide 17)

Questions & Answers

1. In ICANN's Portfolio Management system, the only SSR-related activity that appears is KSK Rollover. Is there another place where SSR-activities are tracked so that the community can see progress on current year activities (for instance the KPI Dashboard seems to be entirely related to the OCTO's work with the technical and public safety communities)?

- DAAR should be in there as well as ITHI for OCTO. Not all activity that could be seen as "SSR-related" lives within the OCTO-SSR team's remit. Items such as compliance and other items that the Review Team is looking at would fall within the relative groups to have included in the system as well.

Did the implementation have the intended effect? How was the assessment conducted?
No. There currently is no mechanism to track the implementation of the SSR Framework.

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

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

SSR2 RT Volunteers: Denise

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.

RECOMMENDATION:

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

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]:

2.2.1 – Identifier Evolution
Description: Track and support the evolution of the Internet's system of unique identifiers through venues such as the IETF, DNS-OARC, W3C, the RIRs, and other relevant bodies.

2.2.2 – Technical Reputation
Description: Measure ICANN's technical reputation across diverse communities and use this to help ICANN develop and improve to grow satisfaction with its performance.

2.2.3 – Security, Stability, and Resiliency of Internet Identifiers
Description: Work to observe, assess and improve the security, stability, and resiliency (SSR) of the Internet's Identifier systems in close collaboration with other ICANN departments and the wider community. This will be achieved through a range of activities including risk awareness and preparedness, measurement and analysis of identifier system behaviors or performance, and cooperative outreach that emphasizes coordination, capability building, and knowledge transfer.
Two of these three portfolios have budgets at the level of portfolio, but no greater detail than that.

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" and that ICANN will "Explore after-event-reports (for relevant threats) that include budget and resource impacts related to managing the event."

Implementation status: 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.

---

[1] See https://www.icann.org/public-comments/fy18-budget-2017-03-08-en

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

- (Phase I) A planning framework and process is 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) Exploration was underway to identify mechanisms that provide more detailed public information on SSR-related budgets and expenditures across multiple ICANN departments. Staff also explored after-event-reports (for relevant threats) that include budget and resource impacts related to managing the event; A template for a public version of these reports has been published and can be found at: https://community.icann.org/display/SSR/Rec+%2320. This report will be published annually for every fiscal year, starting FY18.
- SSR1 implementation report here (slides 58-60)
- SSR2-RT briefing on this recommendation here (slides 30-37)

Questions & Answers

1. Have any after-event reports (for relevant threats) been published that include budget and resource impacts related to managing the event? What would be an example of this kind of after-event-report?

- No after-event reports have been published that include resource impacts related to managing the events. ICANN publishes an information security event log here: https://www.icann.org/cybersecurityincidentlog

2. Provide documentation of, and links to, mechanisms that have been used since 2012 to provide more detailed public information on SSR-related budgets and expenditures across multiple ICANN departments

- Recommendation 20 was implemented in March – April 2017. The 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/CqNYAw

3. Department spending on EBERO?

- The amount of FY17 Professional Services budget ($2.3m) comprises the following main 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

The above items add up to $2.0m. The remaining professional services included in the total are miscellaneous smaller items.

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.

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 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.

SSR2 RT Volunteers: Denise

This recommendation calls for more structured internal process in the development of SSR-related budget decisions, but public material (or the material provided to the review team) does provide evidence at a high level. Greater granularity is needed.

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 observations 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.

Implementation status: 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 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

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

- (Phase I) A planning framework and process is 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) Exploration was underway to identify mechanisms that provide more detailed public information on SSR-related budgets and expenditures across multiple ICANN departments. Staff also explored after-event-reports (for relevant threats) that include budget and resource impacts related to managing the event; A template for a public version of these reports has been published and can be found at: https://community.icann.org/display/SSR/Rec+%2320. This report will be published annually for every fiscal year, starting FY18.
- SSR1 implementation report here (slides 61-63)
- SSR2-RT briefing on this recommendation here (slides 30-37)

Questions & Answers

1. Where is the evidence that a more structured internal process has been developed for SSR budgetary considerations? How do these decisions map onto ICANN's planning framework and process?

- ICANN's planning process ensures that activities planned and budgeted for, including those related to SSR, are identified by specific objectives. More information about the planning process is available here: https://www.icann.org/resources/pages/governance/planning-en

2. Is there a plan for getting public comment on the template prior to using it for publishing information on budget and resource impacts related to SSR events?

- No. There was no plan in place to ask for public comment on the template. The FY18 report has been published and it can be found here: https://community.icann.org/x/DKNYAw

3. Can ICANN provide an update as to the status of phase two (identifying mechanisms that that provide detailed public information on SSR-related budgets), and the steps still to be taken to ensure this recommendation is properly implemented?

- Recommendation 20 was implemented in March – April 2017. The 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/DKNYAw

4. Is there a link to the template described in the staff implementation report?

- Since the template has now been put to use, the actual report for FY18 has replaced the template and it can be found here: https://community.icann.org/x/DKNYAw

5. Where is the budgetary information as it pertains to the SSR? And where is the cost benefit analysis for making these decisions?

- The budgetary information relative to SSR can be found mainly under Objectives 2 and 3 in the Operating Plan and in the Budget by portfolio. As an example, see links to the F19 documents:

FY19 Operating Plan: https://www.icann.org/en/system/files/files/adopted-opplan-fy19-30may18-en.pdf
FY19 Adopted Budget by Portfolio & Project: https://www.icann.org/resources/files/1215649-2018-05-18-en

Did the implementation have the intended effect? How was the assessment conducted?
As with Recommendation 20, SSR related activities do appear in ICANN's annual budget, but at a very high level. SSR1's recommendations 20 and 21 seem 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.

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.

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.

SSR2 RT Volunteers: Denise

This recommendation calls for details related to the gTLD program, but public material (or the material provided to the review team) does not break it out this way. Greater granularity is needed. This remains relevant.

RECOMMENDATION:

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 request to 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 in 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.[1] 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.[2] 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.[3]

---

[1] See https://www.icann.org/ssr-document-archive
[2] https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf
[3] See https://www.icann.org/en/system/files/files/ssr-plan-fy14-06mar13-en.pdf

Implementation status: not implemented.

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

- (Phase I) A planning framework and process is 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) Exploration was underway to identify mechanisms that provide more detailed public information on SSR-related budgets and expenditures across multiple ICANN departments. Staff also explored after-event-reports (for relevant threats) that include budget and resource impacts related to managing the event; A template for a public version of these reports has been published and can be found at: https://community.icann.org/display/SSR/Rec+%2320. This report will be published annually for every fiscal year, starting FY18.
- SSR1 implementation report here (slides 64-66)
- SSR2-RT briefing on this recommendation here (slides 30-37)

Questions & Answers

1. Since the publication of the SSR1 report, what materials have been published by the SSR team that are specific to the implementation of the new gTLD Program? How has that work been budgeted and resourced?

- The OCTO SSR team does not have projects specific to the new gTLD program. These would fall mainly under GDD, which the OCTO SSR team may support.

2. Recommendation 22 is specifically about the new gTLD program. What documentation, specific to the new gTLD Program, on the organization, budget and resources needed to manage SSR issues in this area is available?

- The 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.

Did the implementation have the intended effect? How was the assessment conducted?
SSR1 report indicates that the team saw the new gTLD Program as one having significant SSR related impacts and that it was asking that budget, resource and activity reporting be separated so that the community could see those specific reports. If that conclusion is correct, this Recommendation has not been implemented.

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 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.

SSR2 RT Volunteers: KC

There is money in the budget for these SO/ACs, and their input is a part of the budget planning process. There are operating procedures talk about self-management of conflict-of-interest. ICANN needs to be a place where all points of view are taken into account (as opposed to free from external or internal pressure).

*** Are there any unfunded SSR-related mandates in places other than SSAC or RSSAC? ***

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

- ICANN has in place funding allocated to allow SSAC and RSSAC to conduct work. The support funding has never been linked to, or conditioned by, any performance/output/content evaluation, thus maintaining adequate independence.
- Established processes and procedures for WGs and ACs also support their decisions being reached in an objective manner that is free from external or internal pressure.
- A publicly documented budget process for SO/AC input on the budget is SOP; for example, these requests have been published for FY 15.
- SSR1 implementation report here (slides 67-69)

Questions & Answers

1. Recommendation 23 calls for a mechanism for Working Groups and Advisory Councils to support their decisions in an objective manner that is free from external or internal pressure. Where is such a mechanism documented – specifically regarding the work of SSAC and RSSAC?

- These are documented in the operational procedure. Both committees are undergoing review to improve the work as well. RSSAC Operational Procedures: https://www.icann.org/en/system/files/files/rssac-000-op-procedures-23oct17-en.pdf. SSAC Operational Procedures: https://www.icann.org/en/system/files/files/operational-procedures-27feb18-en.pdf.

kc comments/links: SSAC review document: https://www.icann.org/en/system/files/files/ssac-independent-review-draft-final-15oct18-en.pdf
(now open for public comment: https://www.icann.org/public-comments/ssac-review-final-2018-10-15-en)

RSSAC review documents: https://www.icann.org/resources/reviews/org/rssac
RSSAC intermediate comments: https://www.icann.org/en/system/files/files/rssac-036-14jun18-en.pdf
RSSAC post-process comments: https://www.icann.org/en/system/files/files/rssac-036-14jun18-en.pdf and then https://www.icann.org/en/system/files/files/rssac-041-05oct18-en.pdf
(RSSAC was not satisfied with the review process, indeed their response suggests that they believe the RSSAC review team was not objective; is this in scope?)

kc comment:With respect to RSSAC, the recent review, linked above, suggests the need for considerable additional (unfunded) effort. But it is not clear how much of that will be implemented, or that the expectation is that ICANN fund it. What does RSSAC rep on the committee think? RZERC definitely is multistakeholder, by design (https://www.icann.org/en/system/files/files/revised-rzerc-charter-08aug16-en.pdf)

This looks pretty objective, but I have no idea how ICANN would *ensure* such a thing. Everyone in RSSAC presumably did check with the companies they represented -- why would we want ICANN to stop that? I guess I am not sure how "external" and "internal" are defined in this case.

kc comment:I know that SSAC struggled this year to be responsive to requests for advice on short time frames with inadequate data/research available to inform debate. There was an observation during this year's retreat about the fraction of ICANN's budget directed to SSAC being inadequate given many prevailing and emerging SSR issues and expectations that SSR deliver advice that requires research or synthesis of other research. A related issue: it is not clear how to allocate such funds within SSAC, since much of the work

needed is actual research, and SSAC is a set of volunteers, mostly from industry being subsidized by their employer to participate. To this point, the SSR1 text surrounding this recommendation says: "It would be prudent, however, to ensure that with proper planning, the SSAC and SSAC are given as much time as possible to provide high quality research work and findings." I think SSAC does not generally have the resources to undertake "high quality research work", but this is a statement one should air publicly, since the public/community is the audience for much of SSAC's work products.

A concrete example is the recent NCAP activities, where SSAC proposed a $3M budget to outsource some research they thought would be needed, and my understanding (although it was not too clear to me) was that the ICANN Board thought this 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..). So, I do not know how we could defend "The first recommendation in #22 has been implemented." given what I've witnessed in SSAC. My view may not be representative; I represent a voice for something closer to academic rigor (in analyses to support (or decry) proposed policies potentially disruptive to security, stability, consumer trust) than most appetites in SSAC or the ICANN community. The second sentence in this recommendations touches on this.

kc comment: WRT "ensure decisions are reached in an objective manner that is free from external or internal pressure", I thought the idea of the multistakeholder model is that it's *all* external pressures that will hopefully distill into some reasonable compromise.

I think the fact that our earlier recommendation commentary has emphasized that there are no metrics of success or failure of the new gTLD program to evaluate against, indicates this multistakeholder approach is not "free of external pressures". But the CCT RT report has clearly found some metrics to rigorously use, through which it is impossible to conclude that the gTLD program has been successful from a CCT perspective. What is the SSR2-RT's position on why ICANN did not undertake or fund this sort of exercise itself? My conclusion is that external pressures against this sort of SSR activity prevailed.

kc comment: I'm not sure what to make 2015 budget comment table. Yes, the SO/ACs can comment on the budget, but the process looks disjoint from the community's establishment of SSR priorities, and how "external and internal pressures", however those are measured, are managed.

WRT the operational procedures, there is nothing in the 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. I believe the same is true for RSSAC and RZERC, but in these two cases, it's architected as each person represents a stakeholder (not "objective", but I'm not sure what context "objective" is evaluated; obviously each rootop cares about security and stability of the roots..). It's 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." There are plenty of ICANN staff on the SSAC mailing list, so maybe that helps. But the 'stakeholders' consistently missing from these conversations include victims of DNS abuse, and academic researchers. Given the void, the other stakeholders (aka 'external pressures') prevail.

Note that the SSAC and RSSAC and RZERC are not designed to be 'multistakeholder' in composition. My observation is that they operate in that manner, by nature of their composition.

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

No. The assessment points to the facts that (1) there is money in the budget for these SO/ACs, and their input is a part of the budget planning process (cite to 2015 table); and (2) There are operating procedures that have paragraphs about self-management of conflict-of-interest.

(DM) Recommendation 23 calls for a mechanism for Working Groups and Advisory Councils to support their decisions in an objective manner that is free from external or internal pressure. It is not obvious that such a document or process exists.

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

Yes. But this requires some discussions, because it may be the heart of all the other SSR issues in play. (Management of resources, incentives, and CoIs, in a multistakeholder environment where some stakeholders are observably under-resources and under-represented.) Discuss. :)

(DM) Adequate resources for SSR activities outside of the ICANN Org continue to be an important requirement. The budget, while slightly less opaque than when SSR1 convened, is still not transparent about how working groups and advisory councils are funded.

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

SSR2 RT Volunteers: KC, Scott, Boban, Noorul

ICANN does not have a CSO today. The Office of the CTO, including OCTO SSR, and the Office of the CIO closely coordinate to address the range of ICANN's internal and external SSR responsibilities. There is public information about these roles. More clear and public documentation of the relevant charter, roles, and responsibilities is desirable, including how they coordinate on issues that overlap the organizations.

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

- The Office of the CTO (including OCTO SSR), and the Office of the CIO closely coordinate to address the range of ICANN's internal and external SSR responsibilities. The OCTO 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.
- SSR1 implementation report here (slides 70-72)
- SSR2-RT briefing on this recommendation here (slides 19-22)

No questions & answers.

kc comment: I do not even see the "Chief Security Office Team" mentioned on URLs provided in these slides, much less responsibilities separated by each team. So I can't assess the implementation of this recommendation.

Noorul Ameen: The roles and responsibilities of Chief Security Office Team may be defined in a brief manner.

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

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

Noorul Ameen: The recommendation is still relevant today.

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

SSR2 RT Volunteers: Scott, Boban, Kerry-Ann

A mechanism has been put in place.

*** How does it get incorporated into the strategic plan? ***
[https://www.icann.org/en/system/files/files/strategic-plan-2016-2020-10oct14-en.pdf]

ICANN's Risk Management Methodology and Framework https://www.icann.org/en/system/files/files/summary-risk-management-process-23jan15-en.pdf were presented by ICANN's CFO at the LA Fact Finding Meeting in October 2017. The following processes were highlighted:

- Documented Risk Assessment Process
- Risk Management and Risk Treatment

- Risk Acceptance Criteria and Criteria for Risk Assessment

The methodological approach of the risk management process at ICANN is essentially based on best practices in risk management. It comprises a comprehensive analysis and regular evaluation of threats and an assessment of the probability of their occurrence and impact. The result of the assessment is presented to the Board for further decision.

Note: The result of tech risk assessment is not publicly available. We have signed an NDA to assess the information.

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

- The DNS Risk Management Framework was approved by the Board in Nov. 2013.
- The risk management framework was introduced to the community at ICANN50 and ICANN51, with suggested risks from the community.
- ICANN has an Enterprise Risk Management (ERM) Dashboard that lists risks to be monitored and addressed.
- A DNS Risk Assessment and DNS Resilience Model was published in May 2014.
- An enterprise risk management framework is in place in the ICANN organization.
- SSR1 implementation report here (slides 73-75)
- SSR2-RT briefing on this recommendation here

In terms of sufficiency of addressing the concerns there is still an absence of co-relation of on-going efforts to ensure there is publicly available information to addressing concerns in R 24-26

Questions & Answers

1. Since the Board approval of the 2014 Risk Management Framework provided by an external consultant, what further review, consultation or further work has been done on the approved Framework?

- ICANN org has established a revised risk management framework. This includes thus far establishing an org Risk Management Committee of the org execs, gaining approval for the org's first risk management policy, establishing a Function Risk Liaison Network in which each function is represented in a cross-functional team, and refreshed the risk register, which would be including risks into a formal framework. This framework is moving towards the most important elements of the Risk Management target operating model.

2. Since the publication of the SSR1 Final Report, what mechanisms have been put into place to incorporate near and long-term risks into a formal, strategic Risk Management Framework for ICANN?

- ICANN org has established a revised risk management framework. This includes thus far establishing an org Risk Management Committee of the org execs, gaining approval for the org's first risk management policy, establishing a Function Risk Liaison Network in which each function is represented in a cross-functional team, and refreshed the risk register, which would be including risks into a formal framework. This framework is moving towards the most important elements of the Risk Management target operating model.

3. Please clarify whether the portfolio of the new VP of Enterprise Risk Management extends into risks relating to ICANN's role with regard to the internet's set of unique identifiers, and future threats relating to unique identifiers?

- The risk management framework applies to all ICANN org risks. The role of the VP, Risk Management (not Enterprise Risk Management) is to facilitate the application of the risk management framework.

4. Is there a final DNS risk assessment document (the linked to document is labelled 'draft') https://www.icann.org/en/system/files/files/dns-risk-consultation-28may14-en.pdf, and have there been any updates since 2014?

- There is no final document. DNS risk is included in ICANN's overall risk management.

5. Please provide evidence of briefings to the Board Risk Committee on the risk assessment and proposed mitigation measures, as per Board Resolution dated 21 November 2013 https://features.icann.org/dns-risk-management-framework-report-and-implementation?language=fr, and any follow up arising from such briefings.

- There is no operational "DNS Risk Management Framework." ICANN org now has a risk management framework which covers all risks faced by ICANN org, not just the DNS. Regarding briefings to the BRC about the risk management framework, the BRC meetings have publicly available minutes. Minutes are published to this page: https://www.icann.org/resources/pages/minutes-2014-03-24-en

6. What efforts have been made since 2014 to demonstrate that ICANNs risk management framework follows the standards of transparency and community participation, required by the SSR1?

- We have not yet developed mechanisms to communicate more broadly on risk management. ICANN risk

management will work with ICANN managements and the BRC on next steps.

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 would be valuable to consider the mechanisms to support such review.

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

SSR2 RT Volunteers: Scott, Boban, Kerry-Ann

The DNS Risk Management Framework was approved by the Board in Nov. 2013.

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

- See recommendation 25.
- The Risk Committee of the Board has agreed to the ERM strategy that the organization should pursue, and that this strategy includes at the minimum annual updates on risk assessments, mitigation plans assessment and risk governance.
- SSR1 implementation report here (slides 76-78)
- SSR2-RT briefing on this recommendation here

No questions & answers.

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

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

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

SSR2 RT Volunteers: Scott, Boban, Kerry-Ann

The Risk Management Framework is in place. In the absence of a definition of "comprehensive" by SSR1 or metrics for evaluation, it is very difficult to assess whether this recommendation has been implemented.

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

- See recommendation 25.
- The Risk Committee of the Board has agreed to the ERM strategy that the organization should pursue, and that this strategy includes at the minimum annual updates on risk assessments, mitigation plans assessment and risk governance.
- SSR1 implementation report here (slides 79-81)
- SSR2-RT briefing on this recommendation here

Questions & Answers

1. Please provide details of how the risk management has been staffed since SSR1 recommendations have been adopted by the Board.
   - Board Risk Committee, Risk Management Committee made up of the ICANN org executive team which provides oversight, VP Risk Management, Function Risk Liaisons who are staff members who represent each function for implementing the risk framework, and all organization personnel who own the risks inherent in their activities.
2. The staff report for implementation of SSR1's Recommendations indicates that this Recommendation is

complete. How did staff assess the "comprehensiveness" of the Risk Management Framework to come to this conclusion?

- The ICANN organization staff members that were responsible for implementation of this recommendation are no longer with ICANN. Unfortunately, there is no historical record of how they assess "comprehensiveness" of the Risk Management Framework.

Once again, the staff report simply points to the deliverables for Recommendation 25 as evidence that this recommendation has been completed.

This Recommendation is different from Recommendations 25 and 26 because it asks that the Framework should be "comprehensive." However, SSR1 gave no definition of what "comprehensive" should mean or how that should be evaluated.

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.

Here are two examples of indicative comments:

- "[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

The staff report on the Public Comment process does not address these comments.
In the absence of any definition of "comprehensive" or metrics for evaluation, it is very difficult to judge whether this Recommendation has been implemented.

Did the implementation have the intended effect? How was the assessment conducted?
The implementation was the subject of community criticism and that criticism was not addressed.

<NAVEED> How can we say that it is not addressed when we don't have the definition of what comprehensive is? </NAVEED>

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

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

SSR2 RT Volunteers: Scott, Norm, Noorul

<<< Scott to provide text by mid'ish-October. >>>

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

- Identifier Systems SSR Activities Reporting: https://www.icann.org/news/blog/identifier-systems-ssr-activities-reporting-834ea389-0f61-41d1-809e-b7a458633b87
- As part of our continuing commitment to transparency and accountability, the Identifier Systems SSR department publishes an activities report. The report describes the activities ICANN performs to maintain the security, stability, and resiliency of the Internet's global identifier systems. These activities include collaboration with ICANN, security and operations, and public safety communities, where our staff serves several roles.
- The 1H 2015 activities report highlights ICANNs collaboration and stakeholder activities from January 1 through June 15, 2014. It summarizes activities performed as part of the identifier system SSR threat awareness and preparedness remit. It also provides progress reports on analytics or productivity improvement projects as well.

- Coordinated Vulnerability Disclosure Reporting at ICANN
- Posted the following Blogs:

Threats, Vulnerabilities and Exploits –oh my! 10 August 2015
What is ICANN IIS-SSR? 4 August 2015
Is This a Hack or an Attack? 15 September 2015
Top Level Domain Incident Response Resource Now Available 28 September 2015

- SSR1 implementation report here (slides 83-84)
- SSR2-RT briefing on this recommendation here (slides 36-37).

No questions & answers.

comments:
Noorul Ameen: Coordinated Vulnerability Disclosure Reporting is related to recommendation no. 15.

NR - 3 Identifier Systems SSR Activities reports were posted for the periods 1H2014, 2H2014 and 1H2015. No evidence that these reports continued to be produced. Reports following 1H2015 do not cover incident reporting and handling.

NR - The ccNSO TLDOPS maintains a contact list and mailing list for incident response affecting ccTLDs

DM - Implicit in this recommendation is a focus on threats and incidents related to ICANN's role in the management of the Internet's unique identifiers and responsible distribution of information related to those threats and incidents.

If one of the activities implicit in this Recommendation is the Coordinated Vulnerability Disclosure Reporting, then the concerns related to Recommendation 15 apply.

NR - ICANN has prepared some training materials to assist TLD operators in dealing with security incidents, monitors service levels and has EBERO providers in standby should a registry fail. I have not found similar provisions for registrars.

NR - The GAC's PSWG is charged with the strategic goals of::
1. Develop DNS Abuse and Cybercrime mitigation capabilities
2. Preserve and Improve Domain Registration Directory Service Effectiveness
3. Build Effective and Resilient PSWG Operations
4. Develop Participation in PSWG Work and Ensure Stakeholder Input

NR - https://www.icann.org/groups/ssac

NR - Techday regularly includes technical presentations regarding threats and mitigation to the DNS

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 no public evidence that this has occurred.

There is no public evidence that the ICANN organization conducts ongoing threat detection nor that anyone is tasked with this function. <<<<< someone from SSAC needs to comment on this >>>>

The ICANN community has a number of groups (both open and closed) that actively conducts threat detection including SSAC, RSSAC, TLDOPS, ccNSO incident response WG, and PSWG.

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