Second Security, Stability, and Resiliency Review Team (SSR2)

Public Comment Draft

10 February 2020

ICANN

SSR2 Public Comment Report

Draft report location:
https://www.icann.org/en/system/files/files/ssr2-review-24jan20-en.pdf

Public Comment period open through 04 March 2020 @ 23:59 UTC

See the Public Comment Proceedings for more information:
https://www.icann.org/public-comments/ssr2-rt-draft-report-2020-01-24-en

Workstream Areas

1

Workstream 1:

SSR1 implementation and impact

Section 4.6(c)(iv) of the ICANN Bylaws

2

Workstream 2:

Key security, stability, and resiliency issues within ICANN

Section 4.6(c)(i) of the ICANN Bylaws

3

Workstream 3:

Security, stability, and resilience of the DNS

Section 4.6(c)(iii) of the ICANN Bylaws

4

Workstream 4:

Future challenges

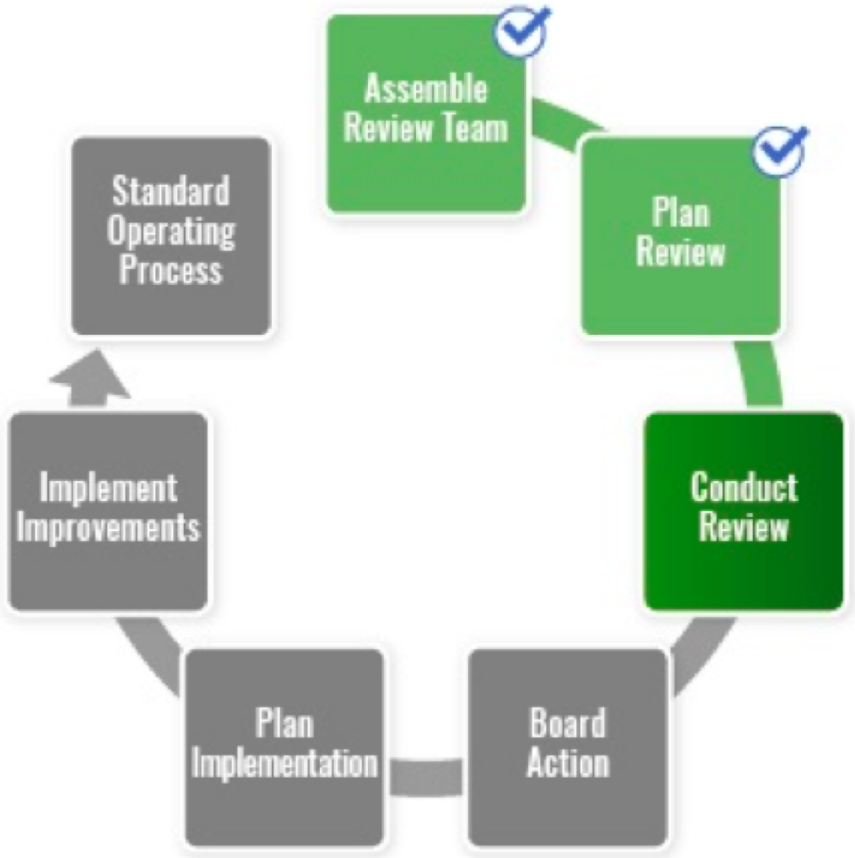
Section 4.6(c)(ii)(A,B,C) of the ICANN Bylaws

SSR2 Review Team

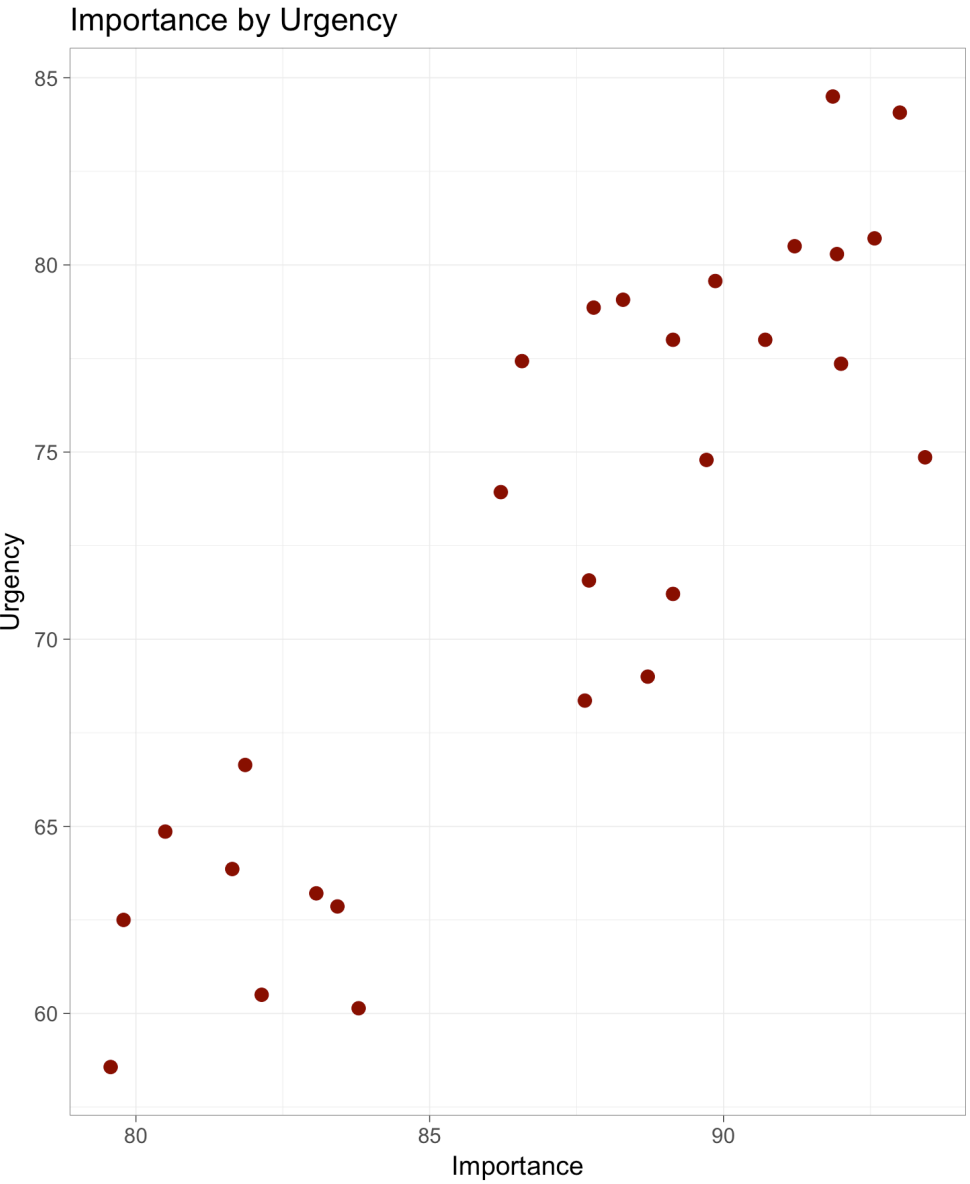
RT Member	SO / AC Affiliation	Region
Alain Aina	ccNSO	AF
Noorul Ameen	GAC	AP
Kerry-Ann Barrett	GAC	LAC
KC Claffy	SSAC	NA
Russ Housley (Chair)	SSAC	NA
Danko Jevtovic	Board	EUR
Žarko Kecić	ccNSO	EUR
Boban Krsic	ccNSO	EUR
Jabhera Matogoro	ALAC	AF
Scott McCormick	GNSO	NA

RT Member	SO / AC Affiliation	Region
Denise Michel (Vice-Chair)	GNSO	NA
Eric Osterweil (Vice-Chair)	RSSAC	NA
Ramkrishna Pariyar	ALAC	AP
Rao Naveed bin Rais	GNSO	AP
Kaveh Ranjbar	Board	EUR
Norm Ritchie	GNSO	NA
Laurin Weissinger (Vice-Chair)	ALAC	EUR

Review Process



Prioritization Process



- Team conducted a survey of SSR2 RT members
- On a scale of 50-100, all recommendations rated 75 or higher, in two clear groupings
- Terminology (low, medium, high) was guided by the definitions used in the CCT report

Recommendations

Review of SSR1 Recommendations

Covered by ICANN Bylaw 4.6(c) …

- 28 SSR1 Recommendations evaluated
- 27 SSR1 recommendations still relevant
  - Most relevant recommendations are not fully implemented

SSR2 recommends going beyond the original SSR1 recommendations in 7 cases

SSR2 Recommendation 1

ICANN org should continue its work to implement all relevant SSR1 Recommendations.

- See page 23 for full recommendation text
- Priority = High

SSR2 Recommendation 2

SSR1 Recommendation 9 – Information Security Management Systems and Security Certifications

- *Improve approach to security certification and audits*

  Priority = High

  See page 23 for full recommendation text

  See also page 71 for findings on the SSR1 recommendation (Appendix D – SSR1 Recommendation 9)

SSR2 Recommendation 3

SSR1 Recommendations 12,15, and 16 - SSR Strategy and Framework, Metrics, and Vulnerability Disclosures

- *Security issue handling and best practice development*

  Priority = High

  See page 24 for full recommendation text

  See also pages 75, 78, and 79 (Appendix D – SSR1 Recommendation 12, 15, and 16)

SSR2 Recommendation 4

SSR1 Recommendations 20 and 22 - Budget Transparency and Budgeting SSR in new gTLDs

- *Improving clarity around budget for SSR*

  Priority = Medium

  See page 24 for full recommendation text

  See also pages 75, 78, and 79 (Appendix D – SSR1 Recommendation 12, 15, and 16)

SSR2 Recommendation 5

SSR1 Recommendations 27 – Risk Management

- *Improving the Risk Management Framework*

  Priority = High

  See page 25 for full recommendation text

  See also pages 91 (Appendix D – SSR1 Recommendation 27)

SSR2 Recommendation 6

Create a Position Responsible for Both Strategic and Tactical Security and Risk Management

- *Recommending the creation of an executive C-Suite position focused on security*

  Priority = High

  See page 27 for full recommendation text

SSR2 Recommendation 7

Further Develop a Security Risk Management Framework

- *Articulate a security risk management framework, including adoption of ISO 31000 "Risk Management"*

  Priority = High

  See page 28 for full recommendation text

SSR2 Recommendation 8

Establish a Business Continuity Plan Based on ISO 22301

- *Establish a BCP for both ICANN and PTI operations based on ISO 22301, to be audited regularly by an external auditor*

  Priority = High

  See pages 29 – 30 for full recommendation text

SSR2 Recommendation 9

Ensure the Disaster Recovery Plan is Appropriate, Functional, and Well Documented

- *Establish a DR plan for ICANN and PTI Operations in line with ISO 27031, to be audited regularly by an external auditor*

  Priority = High

  See page 30 for full recommendation text

SSR2 Recommendation 10

Improve the Framework to Define and Measure Registrar & Registry Compliance

- *Improve compliance with WHOIS/RDS obligations via contracts and SLAs*

  Priority = High

  See pages 37 – 38 for full recommendation text

SSR2 Recommendation 11

Lead Efforts to Evolve Definitions Around Abuse and Enable Reporting Against Those Definitions

- *Starting with the existing definition, continue efforts to establish community consensus for the term "DNS Abuse"*

  Priority = High

  See page 38 for full recommendation text

SSR2 Recommendation 12

Create Legal and Appropriate Access Mechanisms to WHOIS Data

- *Resolve access issues for external parties such as law enforcement around WHOIS/RDS information*

  Priority = High

  See page 39 for full recommendation text

SSR2 Recommendation 13

Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program

- *Improve the overall effectiveness and utility of DAAR*

  Priority = High

  See page 39 for full recommendation text

SSR2 Recommendation 14

Enable Rigorous Quantitative Analysis of the Relationship Between Payments for Domain Registrations and Evidence of Security Threats and Abuse

- *Collect, analyze, and publish pricing data*

  Priority = High

  See page 39 for full recommendation text

SSR2 Recommendation 15

Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse

- *Make SSR requirements mandatory in contracts*

  Priority = High

  See page 40 for full recommendation text

SSR2 Recommendation 16

Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats

- *Offer incentives to encourage SSR within ICANN's contracted parties*

  Priority = High

  See pages 40 – 41 for full recommendation text

SSR2 Recommendation 17

Establish a Central Abuse Report Portal

- *Establish an abuse portal that automatically directs reports to relevant parties*

  Priority = High

  See page 41 for full recommendation text

SSR2 Recommendation 18

Ensure that the ICANN Compliance Activities are Neutral and Effective

- *Audit all compliance activities by a neutral third party, measured against appropriate SLAs*

  Priority = High

  See page 41 for full recommendation text

SSR2 Recommendation 19

Update Handling of Abusive Naming

- *Continue activities to define and measure misleading naming, and then include such data in DAAR when it reaches a level to be considered DNS abuse*

  Priority = High

  See pages 42 – 43 for full recommendation text

SSR2 Recommendation 20

Complete Development of a DNS Regression Test Suite

- *Finish work already started on the test suite*

  Priority = High

  See page 43 for full recommendation text

SSR2 Recommendation 21

Implement the Recommendations from SAC063 and SAC073 and Establish Formal Procedures for Key Rollovers

- *Establish formal KSK rollover process*

  Priority = High

  See page 45 for full recommendation text

SSR2 Recommendation 22

Establish Baseline Security Practices for Root Server Operators and Operations

- *Develop baseline security practices for root servers and recommend appropriate KPIs*

  Priority = High

  See page 46 for full recommendation text

SSR2 Recommendation 23

Accelerate the Implementation of the New-Generation RZMS

- *Increase urgency around deploying the new Root Zone Management System*

  Priority = High

  See page 47 for full recommendation text

SSR2 Recommendation 24

Create a List of Statistics and Metrics Around the Operational Status of the Unique Identifier Systems

- *Create a public list of statistics and metrics to support review of ICANN's unique identifier systems*

  Priority = Medium

  See page 48 for full recommendation text

SSR2 Recommendation 25

Ensure the Centralized Zone File Data Access is Consistently Available

- *Implement the recommendations found in SSAC 97*

  Priority = High

  See pages 48 – 49 for full recommendation text

SSR2 Recommendation 26

Document, Improve, and Test the EBERO Processes

- *Document and automate the Emergency Backend Registry Operator processes*

  Priority = High

  See page 50 for full recommendation text

SSR2 Recommendation 27

Update the DPS and Build Consensus Around future DNSKEY Algorithm Rollovers

- *Prepare for future transition to different digital signature algorithms*

  Priority = Medium

  See page 53 for full recommendation text

SSR2 Recommendation 28

Develop a Report on the Frequency of Name Collisions and Propose a Solution

- *Understand the frequency and nature of name collisions before the next round of gTLDs*

  Priority = Medium

  See page 53 for full recommendation text

SSR2 Recommendation 29

Focus on Privacy and SSR Measurements and Improving Policies Based on Those Measurements

- *Consider privacy impact of new technologies, such as DoH, and how to measure compliance with privacy requirements and principles*

  Priority = High

  See page 56 for full recommendation text

SSR2 Recommendation 30

Stay Informed on Academic Research of SSR Issues and Use That Information to Inform Policy Debates

- *Track developments around SSR in the academic community and disseminate that information to the ICANN community*

  Priority = Medium

  See page 57 for full recommendation text

SSR2 Recommendation 31

Clarify the SSR Implications of DNS-over-HTTPS

- *Commission an independent investigation around the implications of DoH*

  Priority = High

  See page 58 for full recommendation text

SSR2 Report Appendixes

- Definitions and Acronyms
- Suggestions
  - Items specifically targeted towards making future reviews easier to complete
- Process and Methodology
  - How SSR1 Recommendations were evaluated
  - How additional SSR2 work streams were evaluated (ICANN SSR, DNS SSR, and Future Challenges)
- Findings Related to SSR1
- Quoted Text from the ICANN Bylaws, Strategic Objectives and Goals Relevant to the SSR2 report
- Research Data on DNS Abuse Trends
- Table of Alignment Between Specific SSR2 Recommendations and the ICANN Bylaws, Strategic Objectives and Goals

Thank You and Questions

Visit our wiki at **https://community.icann.org/x/AE6AAw**

Submit a public comment: https://www.icann.org/public-comments/ssr2-rt-draft-report-2020-01-24-en