

RSP Technical Questionnaire Review

First IRT Review Session for the RSP Evaluation Program

Gustavo Lozano, Andy Newton

28 November 2023



Agenda

- Brief Overview of the RSP Evaluation Program
- Overview of the Technical Questionnaire
 - Including usage in the RSP Portal
- Security Controls section
- Review and Discussion on Current Comments
- General Discussion
- Next Meeting
 - Review of additional Registry Services and IDN questions

Overview - Why are we doing this?

Recommendation 6.2:

- The Working Group reviewed the fact that where a single RSP provided registry services for multiple TLD applications in the 2012 application round, *the RSP was subject to duplicative evaluation and testing (in some cases hundreds of times)*.
- The Working Group agreed that this **duplicative evaluation and testing could be reduced by establishing a program in which RSPs are evaluated in advance** of an application round opening.

Overview of the RSP Evaluation Program

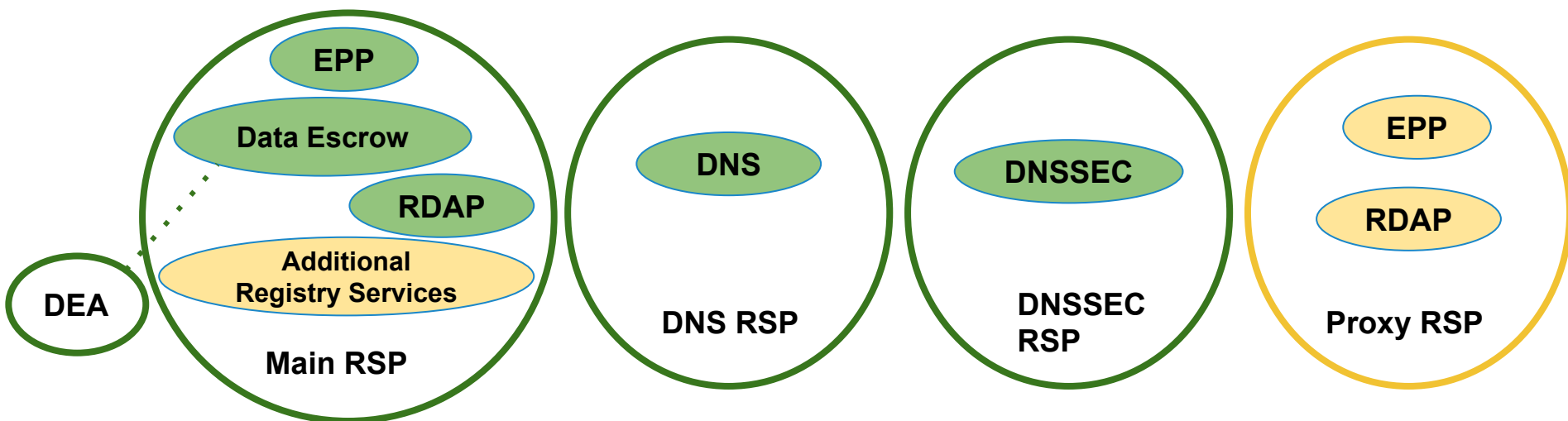
- Allows for the evaluation of RSPs separately from gTLD Registry Operators.
- Accommodates a pre-evaluation phase of RSPs taking place before the gTLD application submission period opens.
- A list of pre-evaluated RSPs will be made available at least six months before the gTLD application submission period opens.
- RSP evaluation can happen either during the pre-evaluation phase or at application evaluation.

Estimated RSP Evaluation Program Timeline

Event	Date
Implementation Review Team Review	Q1 2024
Public Comment	Q1 2024
RSP Evaluation Handbook Publication	Q2 2024
RSP Pre-Evaluation Application Period Begins	Q4 2024
RSP Pre-Evaluation Application Period Ends	Q1 or Q2 2025 (to be determined)
List of Pre-Evaluated RSPs Published	Q4 2025
gTLD Application Submission Period Begins	Q2 2026

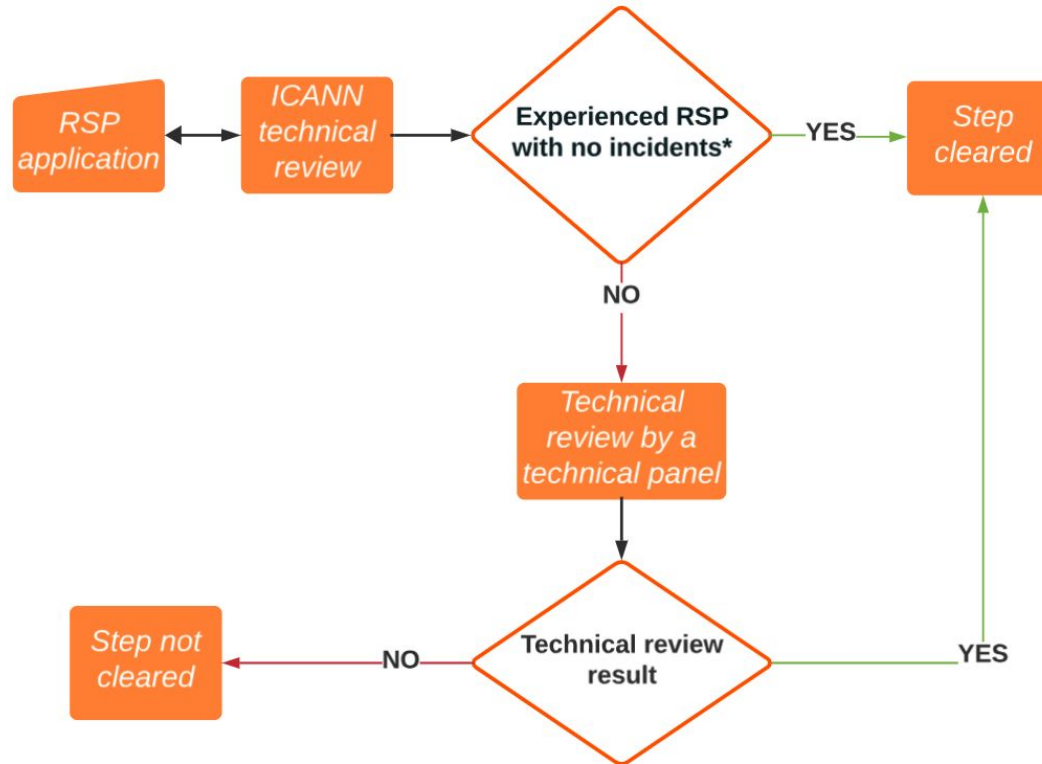
Types of RSPs

- **Per the Subsequent Procedures ODA**, 4 types of RSPs:
 - **Main** (EPP, RDAP, data escrow, and additional Registry Services).
 - **DNS** (DNS service).
 - **DNSSEC** (DNSSEC signing).
 - **Proxy** (“Registration Validation per Applicable Law with Proxy”).
- An organization may be evaluated to be one or more types of RSPs.
- A gTLD applicant must identify at least one RSP for each of the registry critical functions (i.e., Main, DNS, and DNSSEC).



RSP Evaluation - Technical Evaluation

- The following flow chart illustrates the technical evaluation process:



* An RSP operating as a gTLD RSP for the RSP type being evaluated, and there has been no incident that reached the emergency threshold in the past six months for the gTLDs supported by the RSP.

Publication of RSPs

- Answers to all technical evaluation questions for all RSP applications are expected to be made publicly available similar to the last round in 2012.
- A list of all RSPs who passed evaluation will be published six months before the gTLD application period opens.

RSP Types and Technical Questions

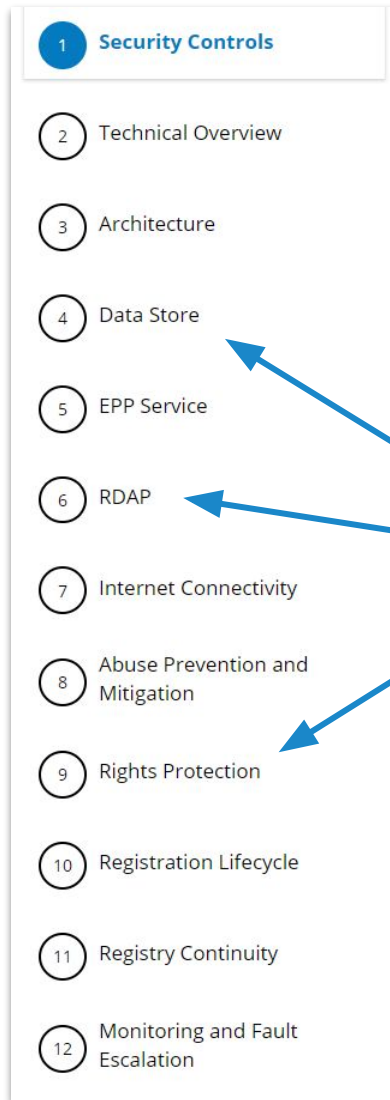
- The questionnaire design uses questions to help the RSP applicant understand what is being asked and minimize the need to generate many pages of information per response.
- Some of the technical questions are repeated across the different types of RSP application.
- The RSP Portal will have a feature to help reduce the need for entering the same information across RSP applications.
- The technical questions are presented in the same order and grouping within the RSP Portal as has been given in the document sent for your review.
- The questionnaire does not need to be filled out in one sitting. Applicants may save their work as needed before submitting the application.

Types of Technical Questions

Yes / No (with optional explanation for No answers)	61.78%
Yes / No / Not Applicable	1.93%
Yes / No with required diagrams (with optional explanation for No answers)	1.16%
Free text with required diagrams	8.49%
Free text with optional diagrams	1.16%
Free text only	25.48%

Diagrams and attachments must be in JPG, PNG, or PDF format.

Screenshot - Wizard




Wizard style progression through sections.

Screenshot - Free text question

- ✓ a. Describe the systems and software relating to the operation of the RSP and the purpose and function for each. This must include, but is not limited to, types of operating systems, application software, programming languages, virtualization environments, network elements, appliances, and sizing requirements. The given list must contain software and systems which are both modern and in common use.

Provide your response below *

0/12000 


Screenshot - Free text with attachment

- ✓ a. Provide a list of all security assessments having received publicly verifiable, 3rd party certification (e.g. ISO 27001) held by the organization and relevant to the registry services under application. For assessments relevant to in-house processes, infrastructure, and systems, specify (a) the year and month the assessment was first conducted or attained, (b) the year and month of the most recent renewal of the assessment (if applicable), (c) the year and month of next planned renewal of the assessment (if applicable), and (d) a URL or some other identifying information or attachment to be used to verify this information. For assessments relevant to third-party vendors (e.g. cloud providers), specify (a) the name of the vendor, (b) the service provided by the vendor, and (c) a URL to the assessment.

Supporting Documents (Optional)

UPLOAD  Drop files here

Provide your response below *

0/6000 

Screenshot - Yes/No question

✓ a. Does or will this RSP comply with RFC 5730?

Select a Choice Below *

Yes No

Screenshot - Yes/No question w/ explanation

- ✓ b. Does or will this RSP have normative, regular, and active practices for the maintenance of hardware relevant to the registry services under application?

Select a Choice Below *

Yes No

Please Provide Additional Details *

0/4000

Security Controls section

Security question

- *Implementation Guidance 27.8: A mechanism(s) should be established to meet the spirit of the goals embodied within Q30b – Security Policy without requiring applicants to provide their full security policy.*
 - a. Provide a list of all security assessments having received publicly verifiable, 3rd party certification (e.g. ISO 27001) held by the organization and relevant to the registry services under application...
 - b. Describe the information security management system (ISMS) implemented by this RSP.

Review and Discussion of Current Comments

<https://docs.google.com/document/d/1HW97Z3uewOGvl9aPiBP7LxLdcWiQq67utVZYmLWp4o8/edit#heading=h.ohvdhsy1nra0>

AoB

Next Steps

- Next review is Tuesday, 12 December.
- That review will include:
 - Comments from this review.
 - Additional Registry Services.
 - IDN questions.

Engage with ICANN



Thank You and Questions

Visit us at icann.org

Email: email



[@icann](https://twitter.com/icann)



facebook.com/icannorg



youtube.com/icannnews



flickr.com/icann



linkedin/company/icann



soundcloud/icann



instagram.com/icannorg