RSSAC037
A Proposed Governance Model for the DNS Root Server System

A Report from the ICANN Root Server System Advisory Committee (RSSAC)
12 June 2018

Executive Summary

In this proposal, the ICANN Root Server System Advisory Committee (RSSAC) presents a governance model for the Domain Name System (DNS) Root Server System (RSS) and its Root Server Operators (RSOs). The audience of this proposal is the Board of Directors of the Internet Corporation for Assigned Names and Numbers (ICANN), the ICANN community, and more broadly, the Internet community.

Today the number of hosts on the Internet is thousands of times larger than when the RSS for the DNS was originally designed. Operational costs for running the service were then miniscule and the value of business conducted on the network was negligible. The network has evolved to billions of hosts, billions of users, new governance structures, and new business models, that all place new expectations on the infrastructure. The RSS, being part of the infrastructure, has largely maintained the same organizational structure throughout all of these changes. It has scaled and adapted to the growth of the network and continues to provide resilient service. However, the time has come for the RSS to adopt new governance structures and business models to meet the more rigorous requirements of governance, accountability, and transparency in this new era.

RSSAC Overview

The RSSAC consists of representatives from the RSO organizations, and liaisons from other ICANN groups and partner organizations involved in the technical and operational management of the root zone. It advises the ICANN community and Board on matters relating to the operation, administration, security, and integrity of the RSS,[1] communicating on matters including:

- Operating the DNS root servers and their multiple instances.
- Gathering requirements and articulating them to those entities engaged in technical revisions of the protocols and common best practices related to the operation of the RSS.
- Engaging in ongoing threat assessment and risk analysis of the RSS and recommending audit activities to assess the status of root servers and the root zone.

As the RSSAC is an Advisory Committee to the ICANN Board, the ICANN community, and the public, the advice of the RSSAC is not binding and should be judged strictly on its merits.

The Root Server System Today

The DNS enables reliable and user-friendly operation of the Internet, and the DNS root service is a vital part of the DNS resolution process, as it provides the starting point for finding resources across the Internet. The current model of the DNS root service has functioned without interruption since its inception.

[1] See "ICANN Bylaws Section 12.2(c)", https://www.icann.org/resources/pages/governance/bylaws-en/#article12

The principles that have enabled the success of this service, and which should remain core principles going forward, include:

1. To remain a global network, the Internet requires a globally unique public namespace.
2. IANA is the source of DNS root data.
3. The RSS must be a stable, reliable, and resilient platform for the DNS service to all users.
4. Diversity of the root server operations is a strength of the overall system.
5. Architectural changes should result from technical evolution and demonstrated technical need.
6. The IETF defines technical operation of the DNS protocol.
7. RSOs must operate with integrity and an ethos demonstrating a commitment to the common good of the Internet.
8. RSOs must be transparent.
9. RSOs must collaborate and engage with their stakeholder community.
10. RSOs must be autonomous and independent.
11. RSOs must be neutral and impartial

These principles are carried forth by the existing RSOs and their collaborative environments (the RSSAC and Root-Ops). The RSOs today operate completely independently under their own good will and funding without any direct oversight by the stakeholders of the service, which is provided solely based on historical trust and integrity. RSSAC has documented much of the history and current structure of root server operations and management, but the governance of the RSS remains largely informal and undocumented.

The Future of Root Server System Governance

The system has worked well since its inception, but no system stands still. Rapid expansion and pervasive use of the Internet has led to the increased importance of the RSS and increased risks to its continued functioning, such as new security threats and user demands. These developments have subsequently led toward stronger needs for accountability, transparency, credible oversight, and continued scalability of the service to meet these demands. Stakeholders of the service must have accountability for its operation and assurance of its reliability and continuity. ICANN, as steward of the IANA functions and the DNS root zone, has evolved considerably in the last few years to meet such needs. Governance of the RSS needs to keep pace.

RSSAC began studying potential replacement models for the current RSS governance model in 2015. The framework presented in this paper is the result of three years of extensive deliberations and modeling by the RSSAC to address the issues of accountability, financial stability, and sustainability of the DNS root service. It is intended to be the initial starting point of a potential framework.

This model continues to build upon the previous principles and proposes an interlocking governance model that consists of the following new components:

1. Secretariat Function (SF)
2. Strategy, Architecture, and Policy Function (SAPF)
3. Designation and Removal Function (DRF)
4. Performance Monitoring and Measurement Function (PMMF)
5. Financial Function (FF)

Each of these components is intended to implement one or more of the principles. Each is described in sufficient detail to act as a starting point for community collaboration. A methodology for estimating the operational costs associated with implementing and maintaining the model is included.

A Way Forward

To support the needed evolution, proposed changes to the governance of the RSS need multistakeholder review and community driven consensus. The proposed model envisions making use of existing ICANN mechanisms for ensuring diverse input to the process (e.g., the Public Comment system, and the various types of groups that might be convened to further develop the model). Wider deliberation on the potential of this model is needed to more broadly vet the proposed components. It is expected that a future ICANN community body will take over further expanding the specifics of the proposal, with the exact form of that body to be decided by the ICANN Board with community input.

Table of Contents

Executive Summary 2

Table of Contents 5

1. Introduction 8

2. Background and Scope 9

  2.1 Motivating Factors 9

  2.2 DNS Root Server System 11

  2.3 Root Zone Management and Resolution 11

3. Guiding Principles of the Root Server System and Root Server Operators 12

4. Root Server System Stakeholders 14

  4.1 Internet Architecture Board and Internet Engineering Task Force 14

  4.2 ICANN Community 15

  4.3 Root Server Operators 16

5. The Model 17

  5.1 Secretariat Function 19

  5.2 Strategy, Architecture, and Policy Function 20

    5.2.1 Streams of Work 20

    5.2.2 Manifestation 21

    5.2.3 Relation to Other Functions 22

  5.3 Designation and Removal Function 22

    5.3.1 Manifestation 23

    5.3.2 Relation to Other Functions 23

  5.4 Performance Monitoring and Measurement Function 23

    5.4.1 Performance Monitoring and Measuring 24

    5.4.2 Evaluation of Potential RSOs 25

    5.4.3 Financial Reporting 25

    5.4.4 Relation to Other Functions 25

  5.5. Financial Function 26

    5.5.1 Strengths 26

    5.5.2 Improvements 27

    5.5.3 Estimated Costs of Developing the Model and Running the RSS 28

5.5.4 Relation to Other Functions 30
6. Example Scenarios 30
6.1 Designate 31
6.1.1 Strategy Architecture and Policy Function 31
6.1.2 Designation and Removal Function 31
6.1.3 Performance Monitoring and Measurement Function 31
6.1.4 ICANN Board 31
6.1.5 IANA Functions Operator 31
6.1.6 Contract Holder 31
6.1.7 Secretariat Function 32
6.2 Voluntary Resignation 34
6.2.1 Strategic Architecture and Policy Function 34
6.2.2 Secretariat Function 34
6.2.3 Contract Holder 34
6.2.4 Performance Monitoring and Measurement Function 34
6.2.5 Designation and Removal Function 34
6.2.6 ICANN Board 35
6.2.7 IANA Functions Operator 35
6.3 Removal for Poor Performance 37
6.3.1 Performance Monitoring and Measurement Function 37
6.3.2 Strategy Architecture and Policy Function 37
6.3.3 Designation and Removal Function 37
6.3.4 ICANN Board 38
6.3.5 IANA Functions Operator 38
6.3.6 Contract Holder 38
6.3.7 Secretariat Function 38
6.4 Catastrophic Shutdown 40
6.4.1 Strategy Architecture and Policy Function 40
6.4.2 Secretariat Function 40
6.4.3 Performance Monitoring and Measurement Function 40
6.4.4 Designation and Removal Function 40

6.4.5 ICANN Board 41
6.4.6 IANA Functions Operator 41
6.4.7 Contract Holder 41
6.5 RSO Goes Rogue 43
6.5.1 Performance Monitoring and Measurement Function 43
6.5.2 Strategy Architecture and Policy Function 43
6.5.3 Designation and Removal Function 43
6.5.4 ICANN Board 43
6.5.5 IANA Functions Operator 44
6.5.6 Secretariat Function 44
6.5.7 Contract Holder 44
7. Conclusion 46
8. Acknowledgments, Dissents, and Withdrawals 46
Dissents 47
Withdrawals 47
9. Revision History 48
9.1 Version 1 48
Appendix A: Glossary of Terms 49
Appendix B. References 50
B.1 RSSAC Publications 50
B.2 RFCs 50

Table of Figures

Figure 1 11
Figure 2 12
Figure 3 18
Figure 4: Designate Scenario 33
Figure 5: Voluntary Resignation Scenario 36
Figure 6: Removal for Poor Performance Scenario 39
Figure 7: Catastrophic Shutdown Scenario 42
Figure 8: RSO Goes Rogue Scenario 45

1. Introduction

The RSS began at the Information Sciences Institute (ISI) in 1984. At the time, it was used to develop the Domain Name System (DNS) and to test early implementations of DNS software. As the software matured, network information centers started to host root servers. The RSS has since expanded to meet the needs of growing interconnected networks – from ARPANET, MILNET, NSFNET – to the global Internet.[2]

Today, the DNS RSS makes the DNS root zone available to all DNS users on the Internet. The servers are currently operated by 12 independent organizations. The system has always provided reliable service to the Internet community. After more than four decades of evolution, today's RSS features root server operators (RSOs) from diverse organizations, increased capacity and connectivity of servers, and more diverse DNS software. The RSS has also added Anycast, DNSSEC, and Internet Protocol version 6 (IPv6) technologies. These technologies have improved the reachability, stability, and security for users of the DNS.

As the global Internet continues to grow and increasingly serves as essential infrastructure that enables international communication and commerce, it is important to look ahead. The RSS needs to evolve so that it remains a reliable, resilient, and sustainable service in the face of increasing traffic and cyberattacks. Important parts of that evolution are ensuring that the operators of the RSS are accountable to their stakeholders, that robust processes exist to designate or remove operators, and that the operators have resources sufficient for its operation.

Since 2015, the Root Server System Advisory Committee (RSSAC) has explored evolving the RSS for long-term sustainability. Through a series of workshops and meetings, the RSSAC has developed an initial evolutionary model (called the *Model* in this report) for the community and the ICANN Board's consideration. This Model identifies authoritative stakeholders of the service, develops criteria to add and remove operators, and recommends accountability for the operators of the system. The Model also proposes a new funding framework.

In this report, we describe the Model. The report is organized as follows:

- Section 2 provides background and scope for the work.
- Section 3 covers the eleven principles that have made the RSS a resilient service to date and that should inform the Model going forward.
- Section 4 defines the stakeholders of the RSS.
- Section 5 outlines five functions envisioned for the Model:
    1. Secretariat Function (SF)
    2. Strategy, Architecture, and Policy Function (SAPF)

[2] For a detailed history, see "RSSAC023: History of the Root Server System"

3. Designation and Removal Function (DRF)
4. Performance Monitoring and Measurement Function (PMMF)
5. Financial Function (FF)

- Section 6 uses several scenarios to illustrate how the functions envisioned in Section 5 interact to designate and remove operators.
- Section 7 presents the conclusion of the report.
- Section 8 contains a list of acknowledgements, dissents and withdrawals to this report.
- Section 9 is a revision history of this report.
- Appendix A presents a glossary of terms used in this report.
- Appendix B links to referenced publications of the RSSAC and the Internet Architecture Board (IAB)/Internet Engineering Task Force (IETF).

2. Background and Scope

This section gives the historical background and discusses how the growth of the Internet has resulted in the need to evolve the DNS root service. It also defines the scope of the proposed Model.

2.1 Motivating Factors

A confluence of events motivates our work.

Until 1997, Dr. Jon Postel designated root server operators. In 1998, ICANN came into existence. ICANN operated the Internet Assigned Numbers Authority (IANA) function with some oversight from the U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA). In 2016, the NTIA ended its oversight of IANA.

Since 1997, 12 operators have delivered the DNS root service. The number of RSOs has remained static, although a few RSOs have changed hands since then.[3] Should a need arise to add or remove operators, it is currently unclear who has the authority to make these changes. Additionally, to ensure the stability and sustainability of the RSS in the long term, we must also address a set of accountability questions.

As the Internet expanded, the DNS root service grew correspondingly in scope and scale. To date, each of the 12 operators has financed its own operations, a model with origins in the natural expansion of the Internet. Delivery of the service has essentially become a mandate for the operators, mostly unfunded by the non-RSO stakeholders of the service. The current model has

[3] Verisign acquired Network Solutions, Inc. in 2000, ICANN took over operation of L-Root from ISI in 2000, and Cogent acquired PSINet in 2002.

worked well for the past few decades because of the integrity, ethics, and global citizenship of the operators.[4]

Increasing reliance on the RSS as an essential infrastructure component has created a need for greater accountability, transparency, and public oversight while maintaining technical excellence. To meet these demands, the current RSS governance model must evolve to accommodate these new realities and new requirements. Stakeholders of the service must have accountability and assurance for the reliability and continuity for the lifetime of the service.

[4] See "RSSAC023: History of the Root Server System"

2.2 DNS Root Server System

The DNS root service spans the global Internet. There are over 1,000 points of access into the DNS RSS, offering a reliable and consistent service to the global Internet population. Figure 1 illustrates the hierarchical nature of DNS resolution. At the top of the hierarchy is the DNS RSS, a global infrastructure with multiple access points for Top-Level Domain (TLD) resolution.

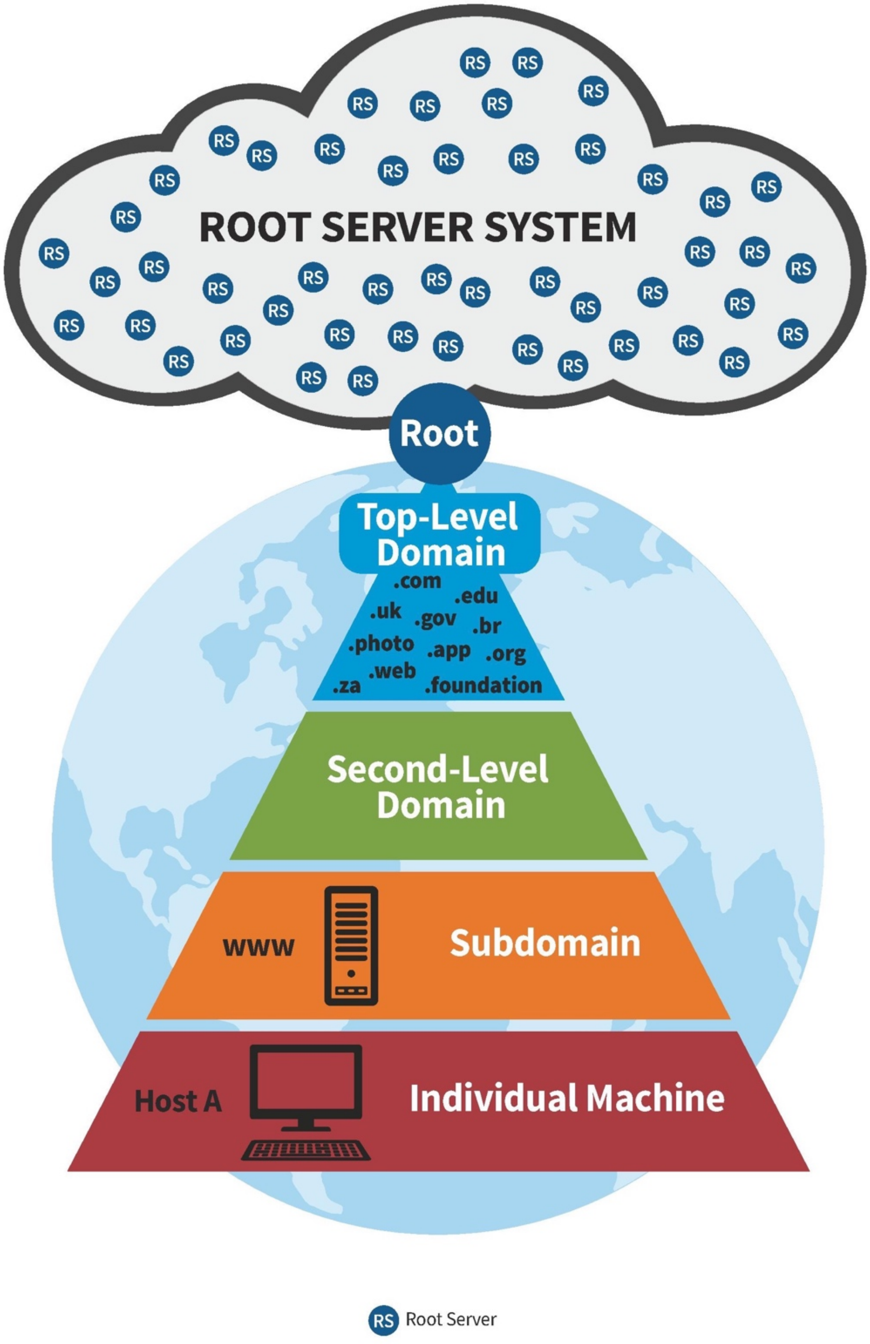

Figure 1

2.3 Root Zone Management and Resolution

Any proposed model must be well-defined and tightly scoped. In Figure 2, the box highlighted in blue depicts the DNS root service – the infrastructure and services operated by the 12 current RSOs. This is also where TLD resolution occurs. The scope of the proposed accountability, performance, funding, and continuity model is confined to what happens in this box.

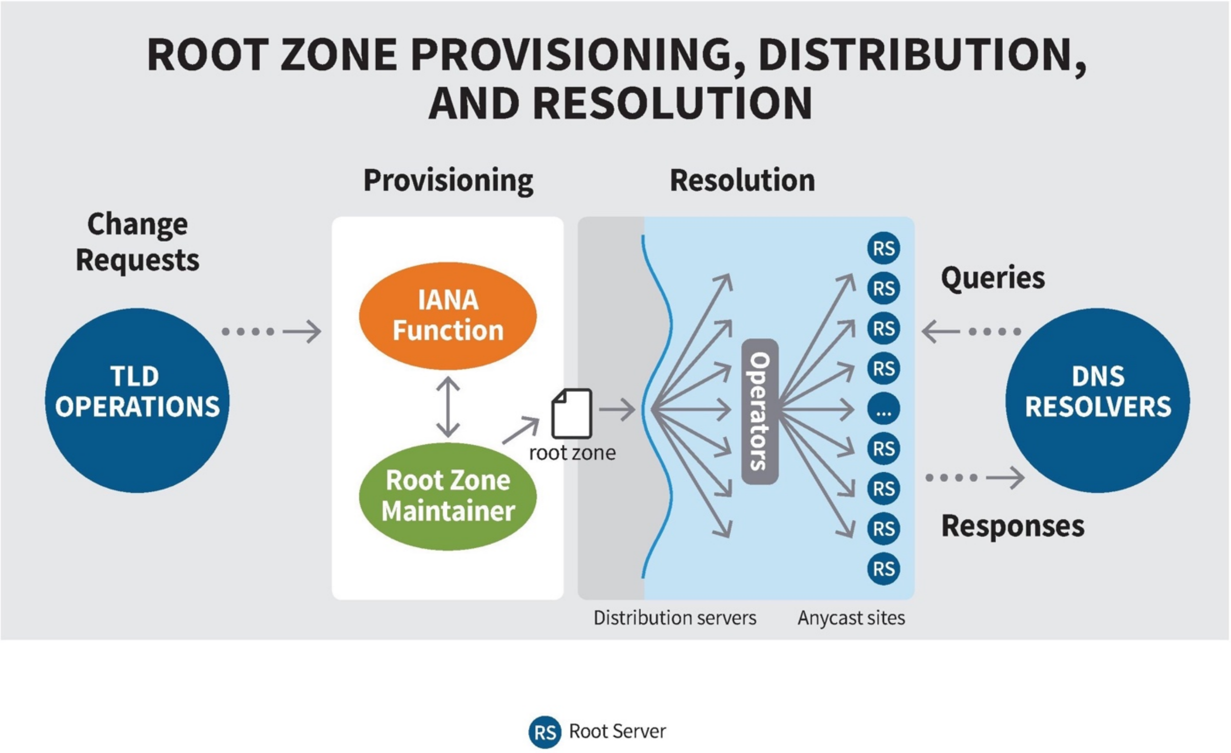

Figure 2

3. Guiding Principles of the Root Server System and Root Server Operators

Eleven principles guide the development and operation of the RSS and RSOs. The RSSAC believes these principles should remain at the core of the Model.

1. **To remain a global network, the Internet requires a globally unique public namespace.** The DNS namespace is a hierarchy derived from a single, globally unique root. This is the key tenet of RFC 2826.[5]
2. **IANA is the source of DNS root data.** RSOs are committed to serving the IANA global root DNS namespace. Root servers provide DNS answers containing *complete* and

[5] See "RFC 2826: IAB Technical Comment on the Unique DNS Root"

unmodified DNS data, including DNS Security Extensions (DNSSEC) data.[6] In addition, IANA maintains the necessary technical information identifying root servers.[7]

3. **The RSS must be a stable, reliable, and resilient platform for the DNS.** The RSOs have a responsibility to provide a high-quality service to the Internet.[8] For example, if an RSO should need to transition operational control to a successor operator, the RSO will provide the Internet community with advance notice and take reasonable measures to facilitate a smooth transition.
4. **Diversity of the root server operations is a strength of the overall system.** Diversity in RSOs' operational models and organizational structures increases the resiliency of the overall system.[9]
5. **Architectural changes should result from technical evolution and demonstrated technical need.** RSOs should embrace emerging technologies affecting the RSS, as long as the Internet's globally unique public namespace is preserved.[10]
6. **The IETF defines technical operation of the DNS.** The IETF and IAB define the protocols underlying DNS implementation in Requests for Comments (RFCs) and other documentation.
7. **RSOs must operate with integrity and an ethos demonstrating a commitment to the common good of the Internet.** RSOs should operate with high moral and ethical standards. They must be committed to sending and responding to traffic without filtering, to serving the IANA global root DNS namespace,[11] and to avoiding conflicts of interest and reciprocal agreements.
8. **RSOs must be transparent.** RSOs must be as transparent as is reasonable without compromising their operational security.
9. **RSOs must collaborate and engage with their stakeholder community.** An RSO must collaborate openly with other operators, participate in group meetings and activities, engage at the IETF in the technical standardization process, and respond to stakeholder questions in a timely manner.
10. **RSOs must be autonomous and independent:** An RSO should have autonomy and independence in architecting and operating their service, while also adhering to standards and service expectations.
11. **RSOs must be neutral and impartial**: An RSO is neutral to the politics of geographic regions and nation states when delivering the DNS root service. The RSO's focus is on provisioning a reliable technical service which knows no political boundaries and

[6] See "RSSAC020: Statement on the Client Side Reliability of Root DNS Data"
[7] See "RSSAC030: RSSAC Statement on Entries in DNS Root Sources"
[8] See "RSSAC016: RSSAC Workshop 2015 Report"
[9] See "RSSAC016: RSSAC Workshop 2015 Report"
[10] See "RSSAC016: RSSAC Workshop 2015 Report"
[11] See "RSSAC020: Statement on the Client Side Reliability of Root DNS Data"

maintains an unbiased position to the politics of any nation state. RSOs must offer DNS service without bias, on the same terms, to users everywhere.

4. Root Server System Stakeholders

A *stakeholder* is a person, group, or organization that has an interest or concern in the duties of an organization. The stakeholders of the RSS are the people, groups, and organizations that have an interest or concern in the proper operation of the RSS.[12] Included as stakeholders are entities with the authority to change the set of operators delivering the service.

For the purposes of this document, the primary stakeholders of the RSS are:

- Internet Architecture Board (IAB) / Internet Engineering Task Force (IETF).
- ICANN community in the form of several of its constituencies.
- Set of current Root Server Operators (RSOs).

4.1 Internet Architecture Board and Internet Engineering Task Force

Although the IAB and the IETF are closely related, they constitute two distinct stakeholders with different scopes and connections to the RSS.

The IAB's current charter is defined in RFC 2850[13], which describes its roles in both the IETF and the Internet Society. The IAB interacts with the RSS in three ways:

- The IAB publishes architecture recommendations and statements as described in RFC 4053[14] that may concern the RSS.

- The IAB convenes groups of experts, either in workshops or programs, who are expected to consider long-term technical issues facing the Internet. A number of these have been relevant to the DNS.

- “The IAB acts as representative of the interests of the IETF and the Internet Society in technical liaison relationships with other organizations concerned with standards and other technical and organizational issues relevant to the worldwide Internet. [...] Individual participants of the IETF are appointed as liaison managers or representatives to other organizations by the IAB.”[15] Among the liaisons it appoints to ICANN are a Board liaison, a liaison to the ICANN Nominating Committee (NomCom), a liaison to

[12] See “RSSAC027: May 2017 Workshop Report”

[13] See "RFC 2850: Charter of the Internet Architecture Board (IAB)"

[14] See “RFC 4053: Procedures for Handling Liaison Statements to and from the IETF"

[15] See "RFC 4052: IAB Processes for Management of IETF Liaison Relationships"

RSSAC, a liaison to the Root Zone Evolution Review Committee (RZERC), and two liaisons to the Technical Liaison Group.[16] These liaisons both convey the results of IETF protocol discussions to these bodies and convey issues raised by those bodies to the IETF. In addition to the above listed liaisons, the IAB manages the IETF relationship with IANA as the protocol parameters registry.

The IETF was created in 1986 and started operating as a standards development organization in 1993. The IETF has oversight for the DNS protocols; a protocol is defined as, "a set of rules governing the exchange or transmission of data between devices."[17] In the context of the DNS, examples of IETF work include defining proper transport on IPv4 and IPv6, various resource records for different uses, and security extensions.

The IETF interacts with the RSS in two ways:

- The IETF facilitates general discussion of the global DNS service and the tools needed for the global DNS. It accomplishes this work through working groups such as the DNS Operations (DNSOP) Working Group. Discussions and formulation of opinions follow the IETF consensus described in RFC 2026 and RFC 2418.[18] The IETF publishes its specifications as RFCs.[19]

- The IETF establishes liaison relationships which the IAB then manages. These IETF liaisons interact with various bodies, including ICANN and its affiliate Public Technical Identifiers (PTI), the IANA Functions Operator. The IAB appoints a liaison to the RSSAC on behalf of the IETF.[20]

4.2 ICANN Community

The *ICANN community* refers to all constituent bodies in ICANN. A significant portion of the ICANN community concerns itself with management of the Internet's top-level domains that are delegated from the unique global DNS root. These groups have an obvious stake in the correct and consistent dissemination of data from the RSS.

As stakeholders, the members of the ICANN community have a vested interest in the resolution of TLDs through the service the RSS provides. This resolution is key to the correct operation of

[16] See "IETF Liaisons", https://www.ietf.org/about/liaisons/

[17] See *Oxford English Dictionary*, 2018 online edition.

[18] See "RFC 2026: The Internet Standards Process – Version 3" and "RFC 2418: IETF Working Group Guidelines and Procedures"

[19] Note that RFCs that predate the existence of the IETF were approved by the Internet Architecture Board.

[20] See "IAB liaison to ICANN Root Server System Advisory Committee (RSSAC)", https://www.iab.org/documents/correspondence-reports-documents/2015-2/iab-liaison-to-icann-root-server-system-advisory-council-rssac/

the global DNS. As such, the ICANN community and in particular, TLD operators, depend on the correct and reliable service of the RSS. This community should have a voice in the issues related to the RSS.

4.3 Root Server Operators

The RSOs collectively operate the global DNS root services corresponding to well-known root service identifiers of the RSS. They are responsible for the day-to-day operations of their respective deployments. The RSOs coordinate operational technical activities and deploy changes required of the RSS over time. They also participate in discussions at organized meetings – or informally using other means of communication. They operate independently as separate organizations. However, they collaborate as needed to ensure that the RSS as a whole operates according to expectations.[21]

RSOs operate as a group without any defined leadership. They use group consensus to make all decisions about the collective operation of the RSS. Each RSO operates independently; no single RSO has authority over any other RSO or over the group as a whole. Now and for the foreseeable future, the service expectations dictate authoritative guidance for individual RSO operations. Each RSO appoints delegates to the RSSAC, which formulates advice about the RSS.

The current set of RSOs come from various organizations: commercial service providers, DNS service providers, universities, software vendors, and government agencies. This set was founded during the initial expansion of the Internet. The RSOs have a strong commitment to the global community to provide a resilient, reliable, and robust service. The support and budget for providing the service comes from the RSOs' parent organizations. As such, the RSOs' own organizations are regarded as stakeholders.

The role of the RSO parent organization is to act as a steward. A steward represents matters and makes decisions for another party even if those decisions might not be in the steward's own best interests. In this context, the specific views of RSO parent organizations as stakeholders vary. However, what is common among the RSO parent organizations is that they accept their responsibilities and do their best to deliver a high quality of service.

[21] "RSSAC001: Service Expectations of Root Servers" and "RFC 7720: DNS Root Name Service Protocol and Deployment Requirements"

5. The Model

Much of RSSAC's work in recent years has focused on the RSS and its operators, a model that evolved out of the growth of the Internet over the past four decades. The RSOs are largely independent, yet tightly bound in mission. The RSSAC workshops have yielded content that defines a potential governance model that is evolutionary, impartial, and sustaining.

The Model is the culmination of RSSAC thought process on this subject. It is to be viewed as the initial framework for a future model built upon the premise of accountability, transparency and continuity.

The Model suggests the creation of these functions within a single framework:

1. Secretariat Function (SF)
2. Strategy, Architecture, and Policy Function (SAPF)
3. Designation and Removal Function (DRF)
4. Performance Monitoring and Measurement Function (PMMF)
5. Financial Function (FF)

Figure 3 depicts the components of the Model.

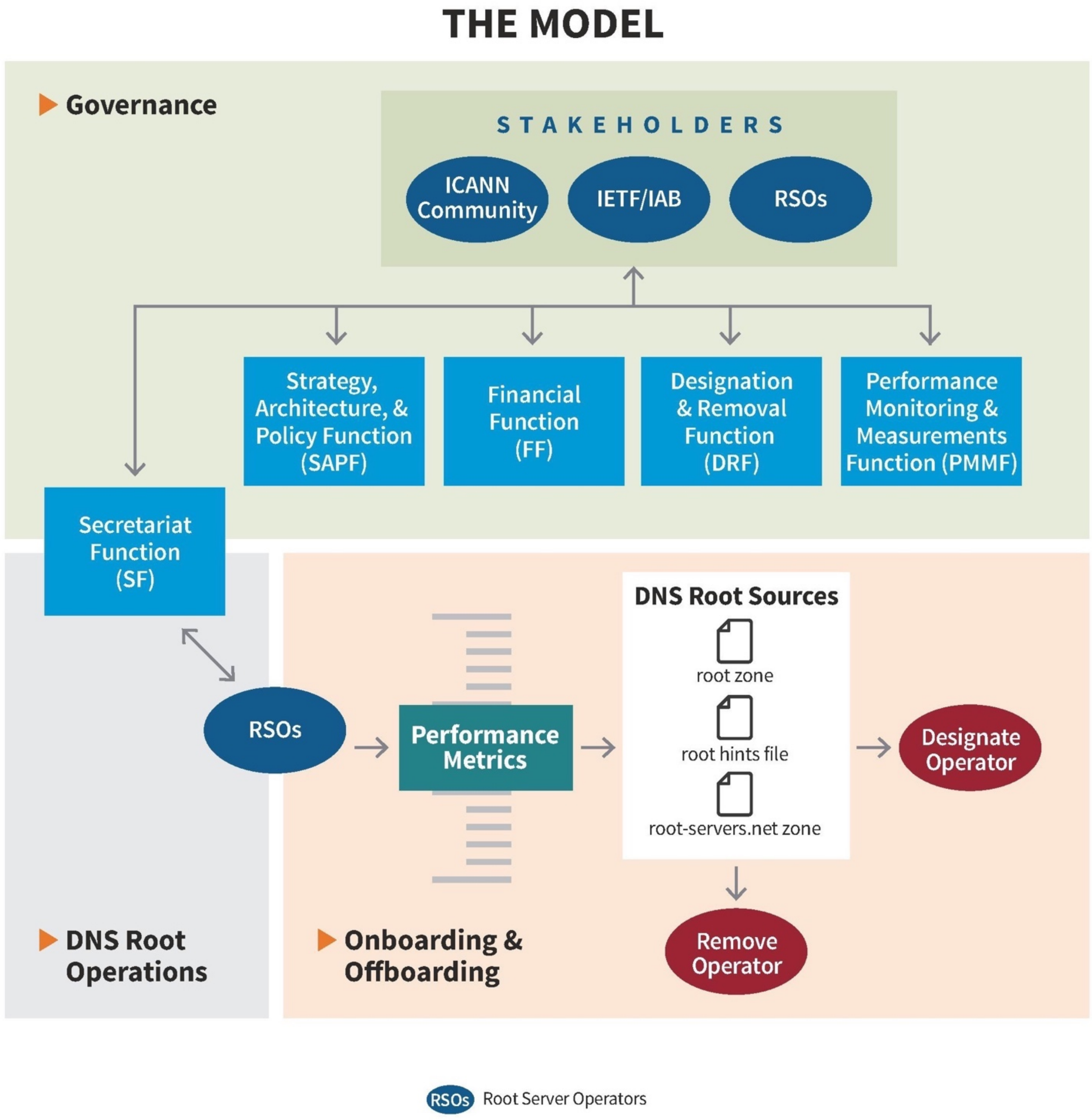

Figure 3

The diagram illustrates the three different constructs of the Model:

- **Governance.** This construct identifies stakeholders and depicts them as the ultimate stewards of the RSS and DNS root service. Architecture elements, operating standards, policy, accountability measures, and designation and removal functions occur within the governance construct under the stewardship of the stakeholders.
- **DNS Root Operations.** This construct illustrates the collective operations of the RSS, along with the coordination of all RSO communication and activities, facilitated by the Secretariat Function (SF).

- **Onboarding and Offboarding.** This construct illustrates the activities associated with onboarding and offboarding RSOs. Onboarding and offboarding activities measure current RSOs and potential new RSOs for performance and eligibility.

Inherent in the Model are three design principles:

- **Separation of Functions.** With much care and deliberation, the Model collocates activities by affinity or separates them to avoid risk. For example, the Model groups the like activities of reporting, evaluating, and compliance under the PMMF, and separates the decision-making DRF from the PMMF to prevent the DRF from influencing the reporting function.
- **Avoidance of Conflicts of Interest.** The functions described in this model will eventually be implemented as various bodies with actual members. The Model accounts for conflicts of interest to ensure that no individual, or an entity they have a relationship with, benefits unfairly from serving on that body. This is generally accomplished by having narrow scopes for each body, requiring transparency in their deliberations, and making sure that no group is composed only of people or organizations with a direct interest in its decisions. For example, the DRF would be constituted of representatives from multiple stakeholder groups.
- **Transparency and Auditability.** The Model includes transparency of decisions and auditability of actions. This naturally leverages the checks and balances of the ICANN ecosystem, to avoid a concentration of influence or functions in any one construct. For example, the SAPF has a mandated responsibility to communicate with stakeholders about strategic, architectural, and policy decisions.

The Model achieves the three main constructs via the three design principles by dividing responsibilities among five functions. The following sections describe the different functions contained in the Model.

5.1 Secretariat Function

The informal and independent manner in which RSOs have traditionally operated has at times been unclear, especially when interacting with entities outside the RSS. Currently, there is no collective channel through which the RSOs can receive requests or publish information. The Model includes a new Secretariat Function (SF) to assist RSOs with certain administrative functions and to create a platform for engagement.

The RSS SF establishes a formal structure where the RSOs are represented. It provides them an official platform from which they can address RSO-related technical issues in an accountable and transparent manner. The SF will be an interface for the Internet community to contact the RSOs.

The precise form of the SF is yet to be determined. However, the RSSAC suggests choosing a model that allows the SF to perform the following functions:

- Performing secretariat and administrative functions to coordinate, facilitate, and support RSO operations and meetings.
- Registering and owning common RSO assets.[22]
- Facilitating and communicating practices related to the RSS.
- Engaging in outreach functions as defined by ICANN and the Internet community.
- Providing a conduit for the Internet community to interact with RSOs.
- Coordinating and providing transparency to the operationalization of appropriate standards (e.g., RSSAC publications and IETF RFCs).
- Assuming new coordination roles that could be defined in the future.

5.2 Strategy, Architecture, and Policy Function

The purpose of the Strategy, Architecture, and Policy Function (SAPF) is to offer guidance on matters concerning the RSS. Numerous emerging technologies could substantially change how the DNS root zone data is delivered. There is growing interest, both technically and politically, in RSS operation and evolution. The SAPF proposes the elements of an architecture based on best practices for global DNS root server operations related to availability, performance, scalability, and security. It also makes recommendations on policy matters to the ICANN community, ICANN Board, and other stakeholders. The SAPF provides a means to capture input and potentially act upon it. The SAPF will consider all of these roles as part of its charter.

5.2.1 Streams of Work

This function is logically divided into three streams of work: strategy, architecture, and policy.

The responsibilities of the *strategy* stream are:

- Coordinating with other stakeholders concerned with the RSS and the root zone in developing a strategic vision for the RSS. Examples of such groups include the ICANN Board, IETF/IAB, SSAC, and RZERC.
- Making recommendations for the appropriate number of RSOs.
- Predicting performance envelopes such as maximum size of the root zone and rate of change from an RSS system-level perspective.
- Strategizing about how to incorporate emerging technologies and how to sunset those technologies that are becoming obsolete.

[22] RSO assets refer to common assets such as the root-servers.org domain name, SSL certificates, and physical assets such as communications equipment.

- Administration and oversight of all processes enacted in the delivery of the Model.

The responsibilities of the *architecture* stream are:

- Ensuring that the guiding principles of the RSS and RSOs remain embedded in technical and operational architectures.
- Defining measurements to ensure that RSOs are meeting a minimum level of performance. Once defined, communicating these measurements to the policy stream to be made actionable for the Performance Monitoring and Measurement Function (PMMF). (For details, see section 5.4.)
- Defining system-wide, externally verifiable metrics to demonstrate that the RSS as a whole is online, serving correct and timely responses to end users. Once defined, communicating these measurements to the policy stream to be made actionable for the PMMF.
- Providing guidance and developing best practices for root server operations based on industry-accepted best practices for the design, capacity, and availability of root servers. This guidance and best practices support the availability, performance, scalability, and security of the RSS.

The responsibilities of the *policy* stream are:

- Defining and articulating policies concerning the RSS. Examples of such policies include; RSS expectations, impacts of significant changes to functionality that the RSS is expected to support, impacts of a significant expansion of the root zone data, and emerging technologies that may impact the functioning of the RSS.
- Gathering input from stakeholders and valued contributors on policy and best practices. This may include handling any grievances concerning an RSO or the RSS.
- Developing evaluation procedures to test the readiness of RSOs and root server instances in cases of outage or overload scenarios.
- Operationalizing the minimum levels of performance developed in the SAPF architecture stream, and communicating this information to the PMMF.
- Operationalizing the system-wide RSS metrics, and collaborating with the PMMF to assess whether the system as a whole meets the defined policy requirements for the RSS.
- Communicating with stakeholders about strategic, architectural, and policy decisions.

5.2.2 Manifestation

The composition of the SAPF needs to include the appropriate skill sets to address the functions of the three streams – strategy, architecture, and policy. The SAPF should include subject matter experts on Internet technologies (with an emphasis on DNS root technology), security, technology architecture, service operations, and policy.

Some of the work to be conducted by the SAPF is currently performed by the RSSAC and the RSSAC Caucus, while other work components of the SAPF are new. The Model envisions that the SAPF will be composed of representatives from the stakeholders, ensuring that the resulting membership contains the breadth and balance of skills needed, including technical, policy and governance expertise.

5.2.3 Relation to Other Functions

The SAPF is responsible for making technical recommendations on the appropriate number of RSOs. The SAPF sends recommendations for an increase or a decrease in the number of RSOs to the Designation and Removal Function (DRF) for potential action. (For details, see section 5.3.)

The SAPF is responsible for defining technical and nontechnical criteria for evaluating the RSOs. The PMMF then uses these criteria for its work. The SAPF is also responsible for defining minimum architectural and operating standards for the RSS and RSOs. The PMMF uses these standards when monitoring and measuring the RSS and RSOs. (For details, see section 5.4.)

5.3 Designation and Removal Function

The Designation and Removal Function (DRF) has the duty to recommend which organizations do, or do not, meet the requirements for serving as RSOs. The DRF has the change management responsibility for the RSS according to policies set by the SAPF. These responsibilities are:

- Receiving applications from organizations willing to be designated as RSOs. In general, the first step is to identify the need to designate a new operator. The DRF will receive applications *only* after establishing a need – to prevent unnecessary work that may never result in a designation.
- Requesting the PMMF to evaluate new RSO candidates on technical and nontechnical merits. Candidates must be evaluated by the PMMF as a prerequisite to being designated as an RSO.
- Reviewing PMMF evaluations of candidate RSOs.
- Recommending the designation of an RSO from a pool of candidates based on the evaluation.
- Handling removal cases where an RSO should no longer operate the root service.
- Participating in accountability efforts by evaluating existing operators for compliance with policies and metrics. The DRF will use information that the PMMF provides to recommend whether to remove or replace any existing RSOs.

5.3.1 Manifestation

The DRF is a reactive committee that responds to a call to action from the SAPF when the need arises to designate or remove an operator. The DRF is invoked as part of the implementation of the Model. After finishing its operational procedures, the DRF has no further tasks until reactivated by the SAPF.

The RSSAC envisions inviting these groups to submit representatives to the DRF:

- Address Supporting Organization (ASO)
- Country Code Names Supporting Organization (ccNSO)
- Generic Names Supporting Organization (GNSO)
- At-Large Advisory Committee (ALAC)
- Governmental Advisory Committee (GAC)
- Security and Stability Advisory Committee (SSAC)
- Root Zone Evolution Review Committee (RZERC)
- Internet Architecture Board (IAB)
- Liaison from the ICANN Board
- Representation from the existing set of RSOs

The designation or removal of an operator is a consequential action, requiring well-defined processes and a carefully constituted DRF. To be effective, the DRF must vote with integrity, relying on data and evidence.

5.3.2 Relation to Other Functions

Although the DRF recommends RSO designations and removals, it does not determine the number of operators required. The SAPF is responsible for making recommendations regarding the appropriate number (or range) of RSOs. If the required number (or range) of RSOs changes, the DRF may be called into action.

The PMMF performs the evaluation of both new and existing RSOs.[23] It evaluates existing operators regularly for compliance with policies, minimum performance requirements, metrics, diversity and ethos. As the need arises, the PMMF evaluates candidate operators. The DRF studies PMMF reports.

5.4 Performance Monitoring and Measurement Function

The Performance Monitoring and Measurement Function (PMMF) provides credible, accurate information on how well the individual RSOs are meeting their commitments, and data on the

[23] For example, see “RSSAC024: Key Technical Elements of Potential Root Operators”

RSS overall performance. The SAPF defines these metrics and thresholds, which the RSOs implement and the PMMF evaluates. In aggregating and monitoring performance metrics, the PMMF performs a supporting watchdog role. This function also evaluates both technical and nontechnical attributes of candidate operators. The PMMF plays a critical role in holding RSOs accountable to the stakeholders.

The PMMF is responsible for:

- Monitoring and measuring RSOs and the RSS against technical and nontechnical standards and expectations that the SAPF develops.
- Evaluating candidate RSOs for the DRF against technical and nontechnical service expectations that the SAPF has developed.
- Reporting if the RSOs are appropriately using the funds they receive from the Financial Function (FF).

While the PMMF is responsible for these activities, it may engage third parties to perform certain tasks as necessary.

5.4.1 Performance Monitoring and Measuring

5.4.1.1 Technical Attributes

The PMMF, with input from the SAPF, evaluates technical metrics and thresholds designed to assess the performance, availability, and quality of service that each RSO provides. When doing so, the PMMF considers the diverse aspects of different RSOs. The RSOs are also expected to self-monitor against the same set of technical attributes.

In cases where measurements indicate that an RSO does not satisfy the defined thresholds, the PMMF will produce a report on the RSO's poor performance. If a documented pattern of poor performance arises, the SAPF may engage the DRF for possible action.

In addition to measurements of individual operators, the PMMF develops and implements techniques for monitoring the RSS. Such monitoring may lead to reports (e.g., IANA reporting on performance[24]) on average response times and availability for the system as a whole.

If systemic disruptions to service occur, the PMMF conducts forensic analyses and produces reports describing the extent and duration of the outages.

[24] See "IANA Reporting on Performance" https://www.iana.org/performance

5.4.1.2 Nontechnical Attributes

The PMMF collects and reviews nontechnical attributes of RSOs. It considers risks to continuity of operation and other risks when measuring and monitoring nontechnical attributes of RSOs. The PMMF determines whether an RSO is stable, using specific criteria that the SAPF provides.

The PMMF confirms the commitment of the RSOs to perform the service, which includes the review of the following commitments:

- Sound business practices around the RSO's service.
- Adherence to RSSAC publications and IETF RFCs.
- Engagements in technical and Internet governance organizations.
- Participation in data and measurement collections.
- Evidence of a strong ethos.
- Contribution to the diversity of the RSS.

Upon review, the PMMF will publish a written assessment of all nontechnical attributes.
The ethos of the RSOs and candidates will be evaluated to maintain a high level of standards among RSOs. The operator ethos, rooted in integrity with strong technical skillsets, and enhanced with an impartial service delivery mindset with a demonstrated desire to do, “what is right for the global Internet community”.

5.4.2 Evaluation of Potential RSOs

The PMMF plays a critical role in evaluating a potential new operator. It conducts the evaluation in tight coordination with both the SAPF and DRF. The SAPF and DRF task the PMMF to review the technical and nontechnical qualifications of an applicant RSO against pre-established standards, as described in section 5.4.1. The PMMF compiles the results of its evaluation into a report and distributes it. The SAPF will develop a thoughtful and well-defined process to ensure that the assessments are thorough, aboveboard, and defensible.

5.4.3 Financial Reporting

The PMMF has the overall responsibility to evaluate the use of funds that RSOs receive from the FF. The PMMF will collect financial reporting data using methods defined by the SAPF to assess fund utilization, then communicate written reports about the use of the funds to the FF and other appropriate bodies.

5.4.4 Relation to Other Functions

Identifying the PMMF as a separate function allows for separation between the PMMF and those bodies that use its results – such as the SAPF, DRF, and stakeholders.

The SAPF creates and communicates the set of standards to the PMMF to monitor and evaluate the RSOs and the RSS. The SAPF can request the PMMF to collect data and perform forensic analyses, and review any grievances concerning an RSO or the RSS.

The DRF relies on the PMMF to provide measurement data about potential new RSOs. The PMMF may also provide data to aid the DRF in any decisions concerning existing RSOs.

If an RSO is determined to be performing below expectations, the SAPF should contact the RSO in question. The RSO must then provide a detailed response that includes a remediation plan with a time frame for any issues. Failure to remediate will be evident from PMMF reports and the SAPF can take action if necessary (e.g., by tasking the DRF).

5.5 Financial Function

The operation of the RSS serves the common good and benefits the global community, as opposed to any one segment of the global Internet population. The evolution of the funding of the service should be viewed from the lens of stakeholders and their global impact. A sustainable model of funding is necessary. This section describes the Financial Function (FF), a fund to be created and governed by the stakeholders to fund operations, research and development, and emergency situations of the RSS.

In examining the aspects of the current RSS, some salient points stand out. These fall into two categories, strengths and improvements.

5.5.1 Strengths

For the past several decades, the evolution of the RSS produced some noteworthy strengths that the Model should sustain:

- Each operator of the service has autonomy in designing the internal technical architecture of its service in adherence to standards. This autonomy has led to a diversity of architectures, which has translated into a strength of the service. The strength is realized in many ways. For instance, when a technical bug or flaw in a system manifests, it does not affect or take down the entire service because RSOs' internal architectures are different. Such architectural diversity has served the community well and is a cornerstone in the security, stability, and resiliency goals of the RSS.
- Operators have autonomy in designing the internal operational architecture of their service. As with the technical architectural diversity, this strength is realized in multiple ways. For example, an unfortunate operational mishap affects one constellation of the

service, but not the service in its entirety. Such diversity in the operational aspects of the RSS further strengthens the service.

- Currently, the RSOs are different organizational types. This level of diversity is a strength, as it adds to the operational resilience in how the service is operated.

5.5.2 Improvements

To date, the RSOs have borne the cost of service operations, mostly with no financial engagement from the non-RSO stakeholders. The operational costs have become an unfunded mandate. During the past four decades, this cost has increased with no commensurate funding for the operators from the service stakeholder beneficiaries. Billion dollar DNS businesses profit from DNS sales and resolution in which the DNS root service is a critical step. However, the RSOs receive no funding to provide the service that supports these industries. Today, the number of Internet users is estimated to be 4.1 billion and increasing.[25] Compounding the challenge, and due in part to the Internet of Things, the Internet is becoming more complex and cyberattacks continue to grow in scale and severity. These realities add to the cost of operating the service.

In light of these facts, it is time to apply some sound economic principles to how the RSS evolves and is funded. It is time to design an RSS Financial Function (FF) that is anchored in the reality of an exponentially growing global Internet. Those entities that the RSS enables need to take responsibility in funding the service that they depend upon.

In studying the current funding model, three key points emerge:

1. The operation of the RSS needs sustainable funding. Sound economic principles of service funding need to be applied in developing such an FF. Stakeholders of the service and relevant parties need to own the process of developing and administering the FF.
2. The FF should provide access to emergency funds should the need arise.
3. As with all technologies, the global DNS will evolve. This technological advancement requires funding for research, development, and testing.

There is a strong belief that sound and healthy funding is critical for robust service design, delivery, and operations.

The Model proposes that the development of the FF should preserve the operator’s autonomy and independence in architecting and operating the service, while requiring adherence to standards and service expectations. It is imperative to decouple the mechanics of the service delivery from the funding of the delivery.

[25] See "Internet World Stats" https://www.internetworldstats.com/stats.htm

This is a prescription for a nuanced service and FF, and includes these key elements:

- Service Level Expectations (SLEs) should exist between the stakeholders that provide funding and RSOs that receive that funding. SLEs are expectations between a service provider and another party. Minimum standards of service levels and expectations will be codified by the SAPF. (e.g., RSSAC001)
- Operators that are financially self-sufficient and choose to opt-out of general funding will establish the integrity of their continued funding by providing information to the PMMF.
- An RSS fund should be created by sourcing funds from numerous entities, including the stakeholders and the ICANN community.
- For funds received, the PMMF will conduct audits to ensure financial accountability for RSO service delivery.
- An appropriate process needs to be developed to grant funding, coupled with a selection committee whose composition includes stakeholders and other relevant entities. Funds could be requested for three reasons: operations, emergencies, and research and development.

5.5.3 Estimated Costs of Developing the Model and Running the RSS

The cost of the Model can be broken down into four components:

1. Investment needed to ensure the current RSS meets the desired operating standards (RSS-CAPEX)
2. Investment needed to implement and kickstart the Model (i.e., establish the various governance functions) (MODEL-CAPEX)
3. Running cost of the RSS (RSS-OPEX)
4. Running cost of the Model (MODEL-OPEX)

The RSSAC suggests the following methodology to calculate the cost of each component:

Investment needed to ensure current RSS meets desired operating capacity (RSS-CAPEX):

- RSSAC suggests an effort to determine the desired service capacity of the RSS.
- The service capacity is measured in terms of three interrelated parameters; Bandwidth, Packets per second, and Queries per second (BPQ).
- The determination of B, P, and Q should be done in collaboration with at least the RSSAC and the RSSAC Caucus, and possibly input from additional technical communities (e.g., SSAC, IAB).
- Using industry standard cost determination methodologies, third-parties should be able to estimate the cost of running the system for any desired service capacity (values of B, P, and Q).

ICANN Board tolerance of risk in system-wide service capacity:

- Resource over-provisioning, measured in BPQ, to handle a reasonably probable attack is something that has to be included in the cost, and is not simple to estimate. This is essentially the cost of risk.
- Ultimately, the ICANN Board will need to determine what level of risk it finds acceptable in terms of desired BPQ. The cost of risk mitigation is inversely proportional to risk tolerance. The board specified risk tolerance will be factored into the overall cost of the system.

Investment needed to implement and kickstart the Model (MODEL-CAPEX):

- The RSSAC suggests a probe of current support operations of similar organizations (e.g. IANA Functions Operator, the ICANN organization, Regional Internet Registries, etc.) to understand the cost required to kickstart the Model, which is estimated to be around 30% of yearly MODEL-OPEX.

Running cost of RSS (RSS-OPEX):

- The outcome of the probe from RSS-CAPEX should provide enough information to calculate this.

Running cost of the Model (MODEL-OPEX):

- Based on our current understanding of each function and since most of the work is staff-based work, the RSSAC suggests using fully loaded FTEs as the main cost indicator. For simplicity of calculations, the RSSAC suggests breaking down the FTEs to two categories: senior project manager and project manager.
- A probe of current support operations of similar organizations (e.g. IANA Functions Operator, the ICANN organization, Regional Internet Registries, etc.) should find the realistic cost of running these operations with given number of staff, this should yield the cost of running such operations per staff category.
- The RSSAC assesses that the SF will require one senior project manager and one project manager.
- The RSSAC assesses that the SAPF will require two senior project managers and two project managers.
- The RSSAC assesses that the DRF will require one senior project manager.
- The RSSAC assesses that the PMMF will require one senior project manager and one project manager.
- The RSSAC assesses that the FF will require one senior project manager and two project managers.
- The Model will also need one year of operating funds in the startup phase as a reserve fund.

- The RSSAC should also work with the FF to establish an annual research and development (R&D) budget.

5.5.4 Relation to Other Functions

The FF works with the individual RSOs to establish contracts that enable independent funding of the RSOs. The FF works with the PMMF to ensure that the RSOs receiving funding are passing financial audits, before allocating funding for the next year. Additionally, the FF interacts with the SAPF to provide funding for the overall RSS.

6. Example Scenarios

The scenarios included here show how the Model outlined in section 5 would operate. Scenarios indicate which functions are activated, and describe the responsibilities and actions of the functions involved. These scenarios are not exhaustive and do not capture all possibilities. Additional implementation work is needed to fully describe the interactions and examine more scenarios.

6.1 Designate

In this scenario, an entity is designated as a new RSO and added to the set of RSOs.

6.1.1 Strategy Architecture and Policy Function

The SAPF is responsible for determining the desired number, or threshold, of RSOs. Once the SAPF determines there is a potential need to designate a new RSO, the SAPF will task the DRF with initiating the process to designate a new RSO.

6.1.2 Designation and Removal Function

Once tasked, the DRF will determine if a designation needs to occur. If so, the DRF will publish an open call for candidate RSOs to apply for designation. Upon receiving the applications from RSO candidates, the DRF will then ask the PMMF to evaluate the candidate RSOs. Finally, based on the evaluation of PMMF reports and potentially other information, the DRF will make a recommendation to the ICANN Board on the designation of a new RSO.

6.1.3 Performance Monitoring and Measurement Function

The PMMF continuously measures the statistical behavior of the various RSOs and the RSS as a whole. The PMMF is also responsible for evaluating candidate RSOs and providing those evaluations to the DRF to aid in its decision making.

6.1.4 ICANN Board

The ICANN Board receives a recommendation from the DRF to designate the selected entity as a new RSO. The ICANN Board will then instruct the IANA Functions Operator to designate the new RSO, instruct the contract holder to explore the possibility of establishing a new contract with the RSO, and inform the SF of the new RSO.

6.1.5 IANA Functions Operator

When instructed to do so by the ICANN Board, the IANA Functions Operator adjusts the DNS root sources to reflect the addition of the RSO in question.

6.1.6 Contract Holder

The contract holder may be required to establish a contract with the newly designated RSO.

6.1.7 Secretariat Function

The SF performs a set of administrative steps when the RSO is added to the DNS root sources. These tasks include adding the RSO to various RSO mailing lists, updating secretariat websites reflecting the designation, and providing access credentials for resources that the secretariat provides to the RSOs.

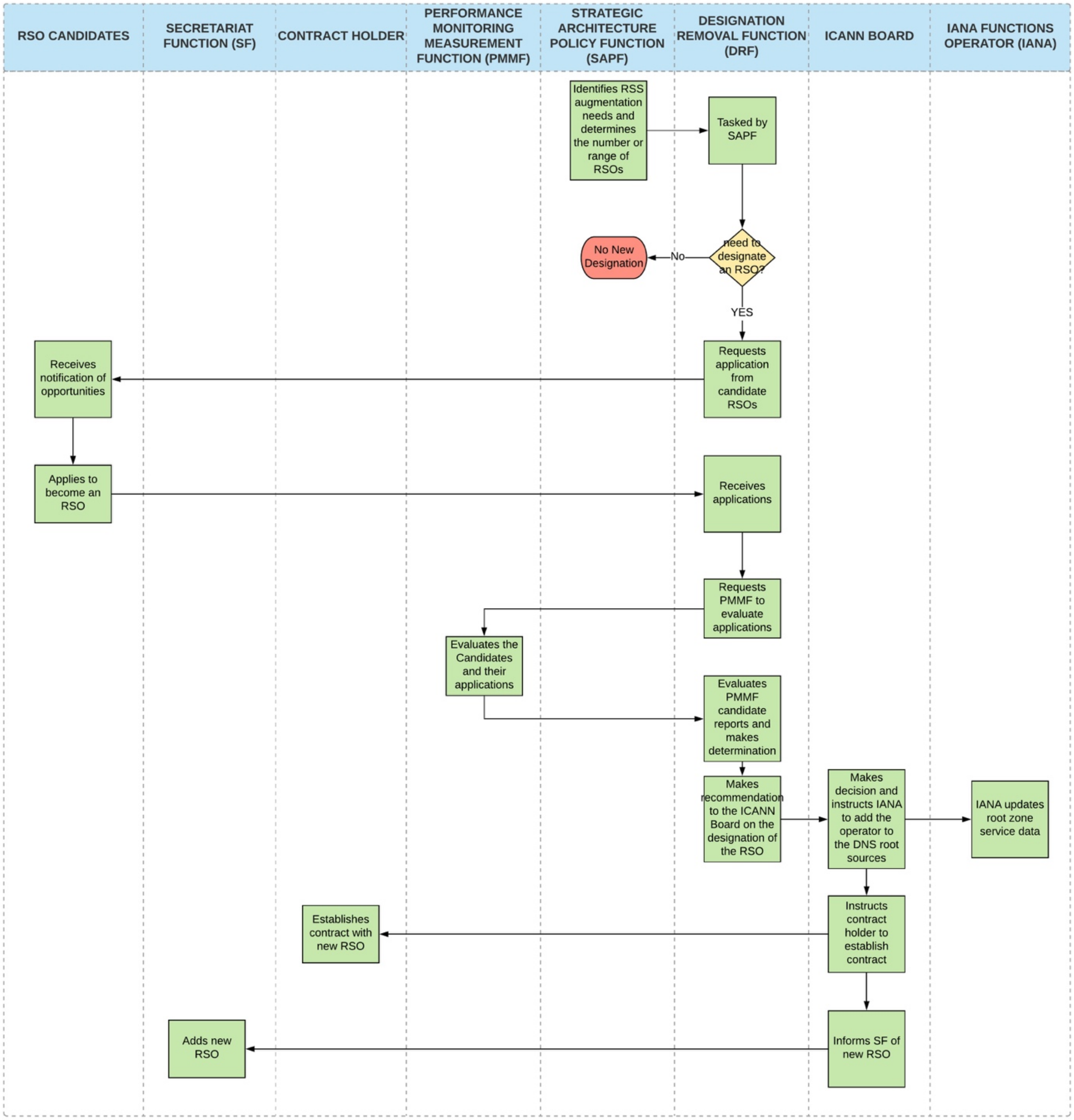
RSO CANDIDATES
SECRETARIAT FUNCTION (SF)
CONTRACT HOLDER
PERFORMANCE MONITORING MEASUREMENT FUNCTION (PMMF)
STRATEGIC ARCHITECTURE POLICY FUNCTION (SAPF)
DESIGNATION REMOVAL FUNCTION (DRF)
ICANN BOARD
IANA FUNCTIONS OPERATOR (IANA)
Identifies RSS augmentation needs and determines the number or range of RSOs
Tasked by SAPF
need to designate an RSO?
No
No New Designation
YES
Requests application from candidate RSOs
Receives notification of opportunities
Applies to become an RSO
Receives applications
Requests PMMF to evaluate applications
Evaluates the Candidates and their applications
Evaluates PMMF candidate reports and makes determination
Makes recommendation to the ICANN Board on the designation of the RSO
Makes decision and instructs IANA to add the operator to the DNS root sources
IANA updates root zone service data
Instructs contract holder to establish contract
Establishes contract with new RSO
Informs SF of new RSO
Adds new RSO

Figure 4: Designate Scenario

6.2 Voluntary Resignation

In this scenario, one of the RSOs advises the SAPF of its intent to discontinue service as an RSO. An RSO may elect to communicate their voluntary resignation via the SF to the SAPF, or directly to the SAPF. This is an orderly shutdown, comparable in many respects to the voluntary termination of the services of a TLD operator.

6.2.1 Strategic Architecture and Policy Function

The SAPF engages the RSO in dialogue to determine the plan of events and informs the other functions for their further action. Upon receiving the verified intention of a given RSO to resign the SAPF notifies the SF, the PMMF, the DRF, and the contract holder if applicable.

The SAPF then reviews any data provided by the PMMF and predicts the impact on the RSS, and if appropriate, makes recommendations concerning that impact.

6.2.2 Secretariat Function

The SF receives the formal notification from the SAPF of the operator's request to resign and notifies the other RSOs. The SF performs a set of administrative steps when the RSO is removed from the DNS root sources. These tasks include removing the RSO from various RSO mailing lists, updating secretariat websites reflecting the removal, and revoking access credentials for resources that the secretariat provides to the RSOs.

6.2.3 Contract Holder

If applicable, the contract holder is provided advance notice that the RSO is discontinuing its service. As part of the formal removal process, the ICANN board will instruct the Contract Holder to terminate any existing contract with the RSO.

6.2.4 Performance Monitoring and Measurement Function

The PMMF may decide to share data on the effect of an RSO discontinuing its service with the other functions (e.g. SAPF and DRF).

6.2.5 Designation and Removal Function

The DRF is tasked to process the RSO resignation by the SAPF. The DRF then acts upon the RSO resignation using information it has received from the SAPF. The DRF then makes a recommendation to the ICANN Board on the removal of an RSO from the DNS root sources[26] on a specified date.

[26] See "RSSAC030: RSSAC Statement on Entries in DNS Root Sources"

6.2.6 ICANN Board

The ICANN Board receives a recommendation from the DRF to remove the resigning RSO. The ICANN Board takes executive action, directing the IANA Functions Operator to make the necessary changes in the DNS root sources on the specified dates. The ICANN Board will also ask the Contract Holder to terminate any existing contract with the RSO.

6.2.7 IANA Functions Operator

When instructed to do so by the ICANN Board, the IANA Functions Operator adjusts the DNS root sources to reflect the removal of the RSO that has resigned.

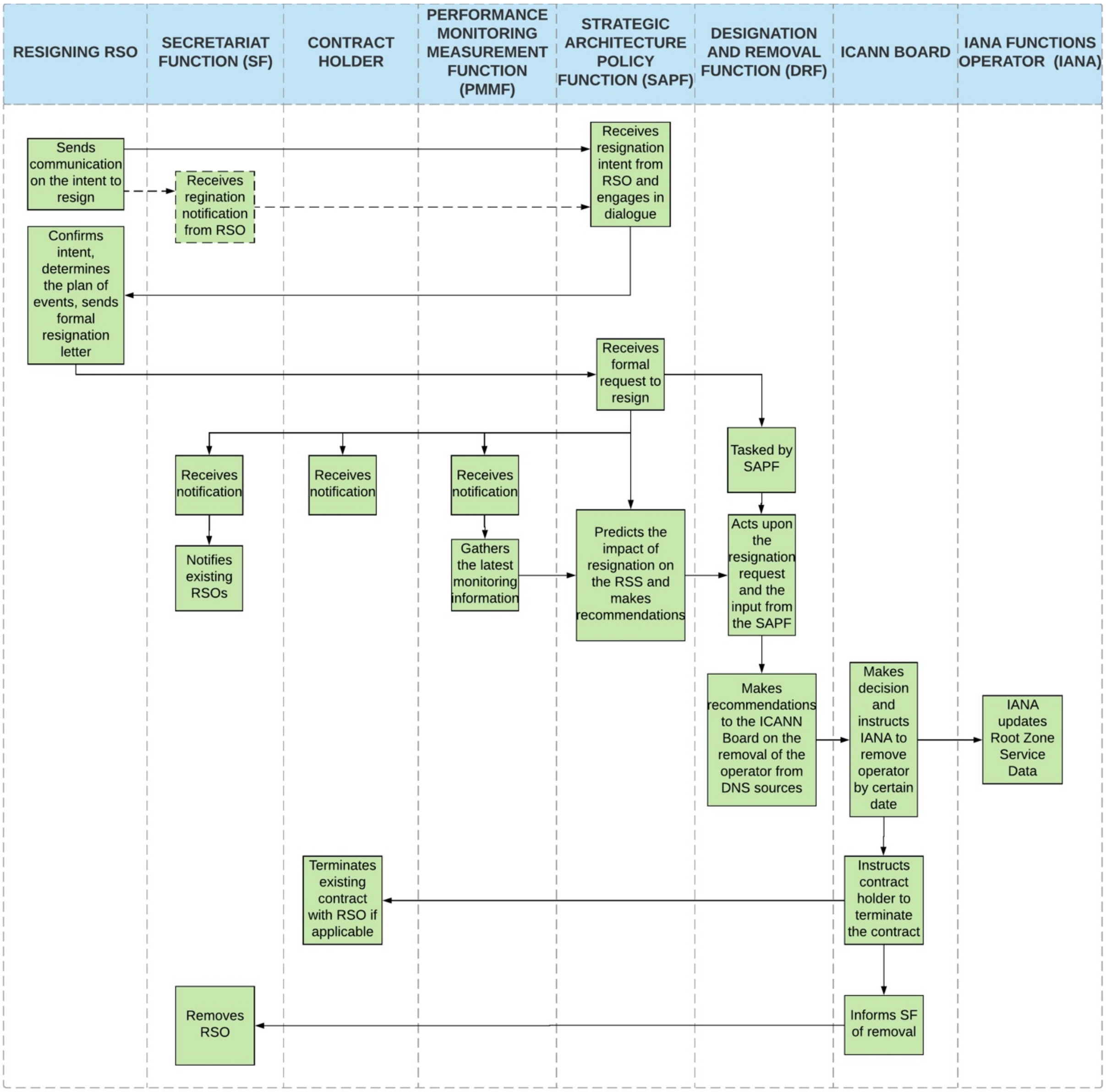
RESIGNING RSO
SECRETARIAT FUNCTION (SF)
CONTRACT HOLDER
PERFORMANCE MONITORING MEASUREMENT FUNCTION (PMMF)
STRATEGIC ARCHITECTURE POLICY FUNCTION (SAPF)
DESIGNATION AND REMOVAL FUNCTION (DRF)
ICANN BOARD
IANA FUNCTIONS OPERATOR (IANA)
Sends communication on the intent to resign
Receives regination notification from RSO
Receives resignation intent from RSO and engages in dialogue
Confirms intent, determines the plan of events, sends formal resignation letter
Receives formal request to resign
Tasked by SAPF
Receives notification
Receives notification
Receives notification
Notifies existing RSOs
Gathers the latest monitoring information
Predicts the impact of resignation on the RSS and makes recommendations
Acts upon the resignation request and the input from the SAPF
Makes recommendations to the ICANN Board on the removal of the operator from DNS sources
Makes decision and instructs IANA to remove operator by certain date
IANA updates Root Zone Service Data
Terminates existing contract with RSO if applicable
Instructs contract holder to terminate the contract
Removes RSO
Informs SF of removal

Figure 5: Voluntary Resignation Scenario

6.3 Removal for Poor Performance

In this scenario, it is determined that one of the existing RSOs has failed to meet the expectations listed in RSSAC001. Action must be taken for the good of the Internet. The motivation for this scenario is an accountability duty to the stakeholders. The Internet is strengthened when it does not depend on failing infrastructure.

6.3.1 Performance Monitoring and Measurement Function

The PMMF continuously measures the statistical behavior of the various RSOs and the RSS as a whole. In this case, its data clearly points to a failing RSO. When the PMMF identifies that an RSO is not performing adequately, it produces a report and notifies the SAPF.

Alternatively, a performance problem may be reported to the SAPF by an Internet community entity. The SAPF would then notify the PMMF of the issue so that they can alter their monitoring as necessary to assist with the investigation.

The DRF may ask the RSO to improve their performance. If so, the PMMF will be responsible for reporting on changes to the RSO's performance.

6.3.2 Strategy Architecture and Policy Function

Upon receiving notification from the PMMF, the SAPF will task the DRF to study the performance of the RSO in question.

If the RSO in question fails to remediate successfully as determined by the DRF, the SAPF will determine any predicted impact of removal prior to the RSO being removed.

6.3.3 Designation and Removal Function

Upon being tasked by the SAPF to act on the RSO that is not performing adequately, the DRF evaluates the situation based on data from the PMMF reports and potentially other sources.

The DRF then determines whether the RSO is in a critical state. If the DRF determines that the RSO is in a critical state it will request the RSO to improve its performance by a specified date in order to avoid being removed. If the RSO is not in a critical state the DRF will request that the RSO improve its performance.

If the RSO was requested to improve its performance by a specified date and it fails to do so as determined by the DRF, the DRF will recommend to the ICANN Board that the RSO in question be removed.

6.3.4 ICANN Board

The ICANN Board may receive a recommendation from the DRF to remove the RSO for poor performance. The ICANN Board takes executive action, directing the IANA Functions Operator to make the necessary changes in the DNS root sources on the specified dates.

6.3.5 IANA Functions Operator

When instructed to do so by the ICANN Board, the IANA Functions Operator adjusts the DNS root sources to reflect the removal of the RSO in question.

6.3.6 Contract Holder

If applicable, the contract holder will terminate its contract with the RSO after instructed to do so by the ICANN Board.

6.3.7 Secretariat Function

The SF is notified by the ICANN Board of the date on which the RSO in question is to be removed. The SF performs a set of administrative steps when the RSO is removed from the DNS root sources. These tasks include removing the RSO from various RSO mailing lists, updating secretariat websites reflecting the removal, and revoking access credentials for resources that the secretariat provides to the RSOs.

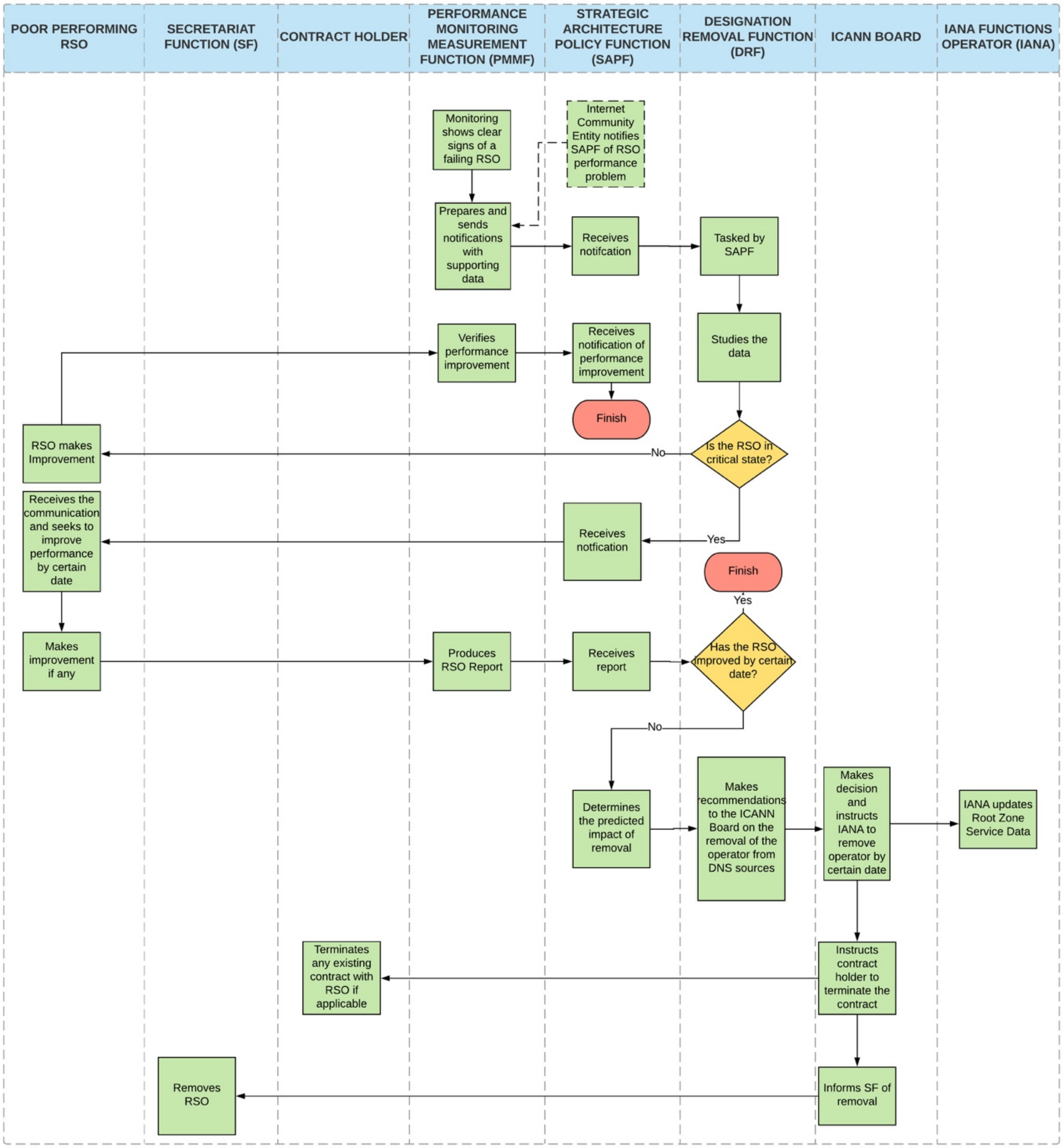
POOR PERFORMING RSO
SECRETARIAT FUNCTION (SF)
CONTRACT HOLDER
PERFORMANCE MONITORING MEASUREMENT FUNCTION (PMMF)
STRATEGIC ARCHITECTURE POLICY FUNCTION (SAPF)
DESIGNATION REMOVAL FUNCTION (DRF)
ICANN BOARD
IANA FUNCTIONS OPERATOR (IANA)
Monitoring shows clear signs of a failing RSO
Internet Community Entity notifies SAPF of RSO performance problem
Prepares and sends notifications with supporting data
Receives notifcation
Tasked by SAPF
Studies the data
Verifies performance improvement
Receives notification of performance improvement
Finish
Is the RSO in critical state?
No
RSO makes Improvement
Yes
Receives notification
Receives the communication and seeks to improve performance by certain date
Finish
Yes
Makes improvement if any
Produces RSO Report
Receives report
Has the RSO improved by certain date?
No
Determines the predicted impact of removal
Makes recommendations to the ICANN Board on the removal of the operator from DNS sources
Makes decision and instructs IANA to remove operator by certain date
IANA updates Root Zone Service Data
Terminates any existing contract with RSO if applicable
Instructs contract holder to terminate the contract
Removes RSO
Informs SF of removal

Figure 6: Removal for Poor Performance Scenario

6.4 Catastrophic Shutdown

In this scenario, one RSO experiences a catastrophic shutdown that either permanently or temporarily causes their root operations to cease. The detection probably comes in a communication from the RSO indicating that the event has occurred or the impact will be detected by the monitoring functions of the PMMF. As such, it is similar to the *Voluntary Resignation* scenario in 6.2, except that the interval between notice and non-operation is greatly shortened. It is also similar to the *Removal for Poor Performance* scenario in section 6.3, except the RSO has ceased operations with potential of resuming operations at a later date.

6.4.1 Strategy Architecture and Policy Function

The SAPF first engages in dialogue with the failing RSO to determine the severity of the outage.

If the outage is recoverable, the SAPF will request the RSO in question work to resume operations by a specified date and follow a set of remediation steps outlined in the *Removal for Poor Performance scenario*. If the outage is not recoverable it will task the DRF to initiate the RSO removal process. The SAPF will also inform the SF, the contract holder and the PMMF of the outage.

6.4.2 Secretariat Function

The SF relays information between the SAPF and the RSOs concerning the shutdown. The SF will notify the RSOs of the catastrophic shutdown experienced by an RSO. Once the ICANN Board acts on the DRF recommendation that the RSO that has ceased operations should be removed, the SF will remove the RSO. The SF performs a set of administrative steps when the RSO is removed from the DNS root sources. These tasks include removing the RSO from various RSO mailing lists, updating secretariat websites reflecting the removal, and revoking access credentials for resources that the secretariat provides to the RSOs.

6.4.3 Performance Monitoring and Measurement Function

The PMMF will either be notified by the SAPF of the RSO's catastrophic shutdown or they will have detected the failure via their monitoring activities. The PMMF will produce a report on any perceived impact and share it with the other functions (e.g. SAPF and DRF).

6.4.4 Designation and Removal Function

If the outage is not recoverable the SAPF will task the DRF to initiate the RSO removal process. The DRF will recommend to the ICANN Board the removal of the RSO in question from the DNS root sources on a specified, perhaps immediate, date.

6.4.5 ICANN Board

The ICANN Board receives a recommendation from the DRF to remove the RSO that has ceased operations. The ICANN Board takes executive action, directing the IANA Functions Operator to make the necessary changes in the DNS root sources on the specified dates. It also instructs the SF to remove the RSO in question and the contract holder to terminate any contract it has with the RSO.

6.4.6 IANA Functions Operator

When instructed to do so by the ICANN Board, the IANA Functions Operator adjusts the DNS root sources to reflect the removal of the RSO in question.

6.4.7 Contract Holder

The contract holder is informed of the failure by the SAPF and, if applicable, will terminate its contract with the RSO after instructed to do so by the ICANN Board.

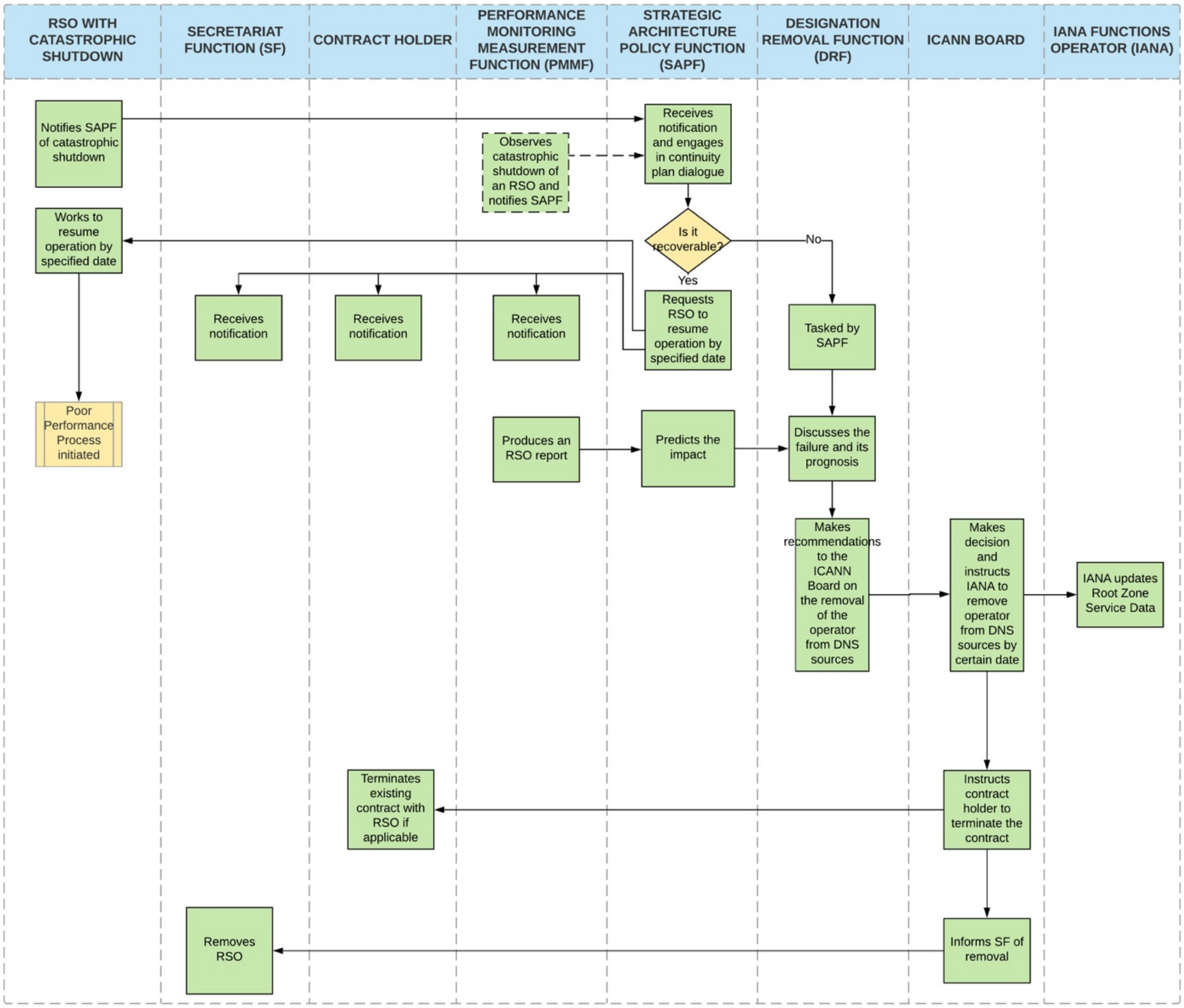
RSO WITH CATASTROPHIC SHUTDOWN
SECRETARIAT FUNCTION (SF)
CONTRACT HOLDER
PERFORMANCE MONITORING MEASUREMENT FUNCTION (PMMF)
STRATEGIC ARCHITECTURE POLICY FUNCTION (SAPF)
DESIGNATION REMOVAL FUNCTION (DRF)
ICANN BOARD
IANA FUNCTIONS OPERATOR (IANA)
Notifies SAPF of catastrophic shutdown
Observes catastrophic shutdown of an RSO and notifies SAPF
Receives notification and engages in continuity plan dialogue
Is it recoverable?
No
Yes
Works to resume operation by specified date
Receives notification
Receives notification
Receives notification
Requests RSO to resume operation by specified date
Tasked by SAPF
Poor Performance Process initiated
Produces an RSO report
Predicts the impact
Discusses the failure and its prognosis
Makes recommendations to the ICANN Board on the removal of the operator from DNS sources
Makes decision and instructs IANA to remove operator from DNS sources by certain date
IANA updates Root Zone Service Data
Terminates existing contract with RSO if applicable
Instructs contract holder to terminate the contract
Removes RSO
Informs SF of removal

Figure 7: Catastrophic Shutdown Scenario

6.5 RSO Goes Rogue

In this scenario, one RSO has intentionally misbehaved and it must be investigated for potential removal. Examples of misbehavior might include the RSO intentionally not serving the correct contents of the root zone file, the RSO not answering queries from selected entities, or the RSO misusing funds from the FF. If such an issue were to occur, it is important that quick action be taken to limit the adverse impact on the Internet.

6.5.1 Performance Monitoring and Measurement Function

The PMMF continuously measures the statistical behavior of the various RSOs and the RSS as a whole. Through its monitoring, the PMMF is expected to be the first function to observe that a given RSO has done something which may be considered rogue behavior. However, it is also possible that the RSO's intentional acts may be reported to the SAPF before being noticed by the PMMF. In this case, the SAPF may provide information to the PMMF to assist in any ongoing analysis.

6.5.2 Strategy Architecture and Policy Function

Upon being informed by the PMMF that an RSO is not adhering to expectations, the SAPF will determine if the RSO requires immediate removal. If not, the SAPF will communicate with the RSO to determine if the RSO will remediate. If the RSO is non-responsive, or the SAPF determines the issue is deliberate or persistent, the SAPF will task the DRF to investigate removal of the RSO in question.

If the RSO is responsive and willing to resolve the issue the SAPF will work with the RSO to establish a remediation plan and a timeline for remediation.

6.5.3 Designation and Removal Function

If the SAPF discovers that the RSO is non-responsive or determines that the issue is deliberate or persistent, the SAPF will task the DRF to initiate the RSO removal process. As a consequence, the DRF may make a recommendation to the ICANN Board to remove the offending RSO.

6.5.4 ICANN Board

The ICANN Board receives a recommendation from the DRF to remove the rogue RSO. The ICANN Board takes executive action, directing the IANA Functions Operator to make the necessary changes in the DNS root sources on the specified dates. It also instructs the SF to remove the RSO in question, and the contract holder to terminate any contract it has with the RSO.

6.5.5 IANA Functions Operator

When instructed to do so by the ICANN Board, the IANA Functions Operator adjusts the DNS root sources to reflect the removal of the RSO in question.

6.5.6 Secretariat Function

The SF is notified by the ICANN Board of the date on which the RSO in question is to be removed. The SF performs a set of administrative steps when the RSO is removed from the DNS root sources. These tasks include removing the RSO from various RSO mailing lists, updating secretariat websites reflecting the removal, and revoking access credentials for resources that the secretariat provides to the RSOs.

6.5.7 Contract Holder

The contract holder, if applicable, will terminate its contract with the RSO after instructed to do so by the ICANN Board.

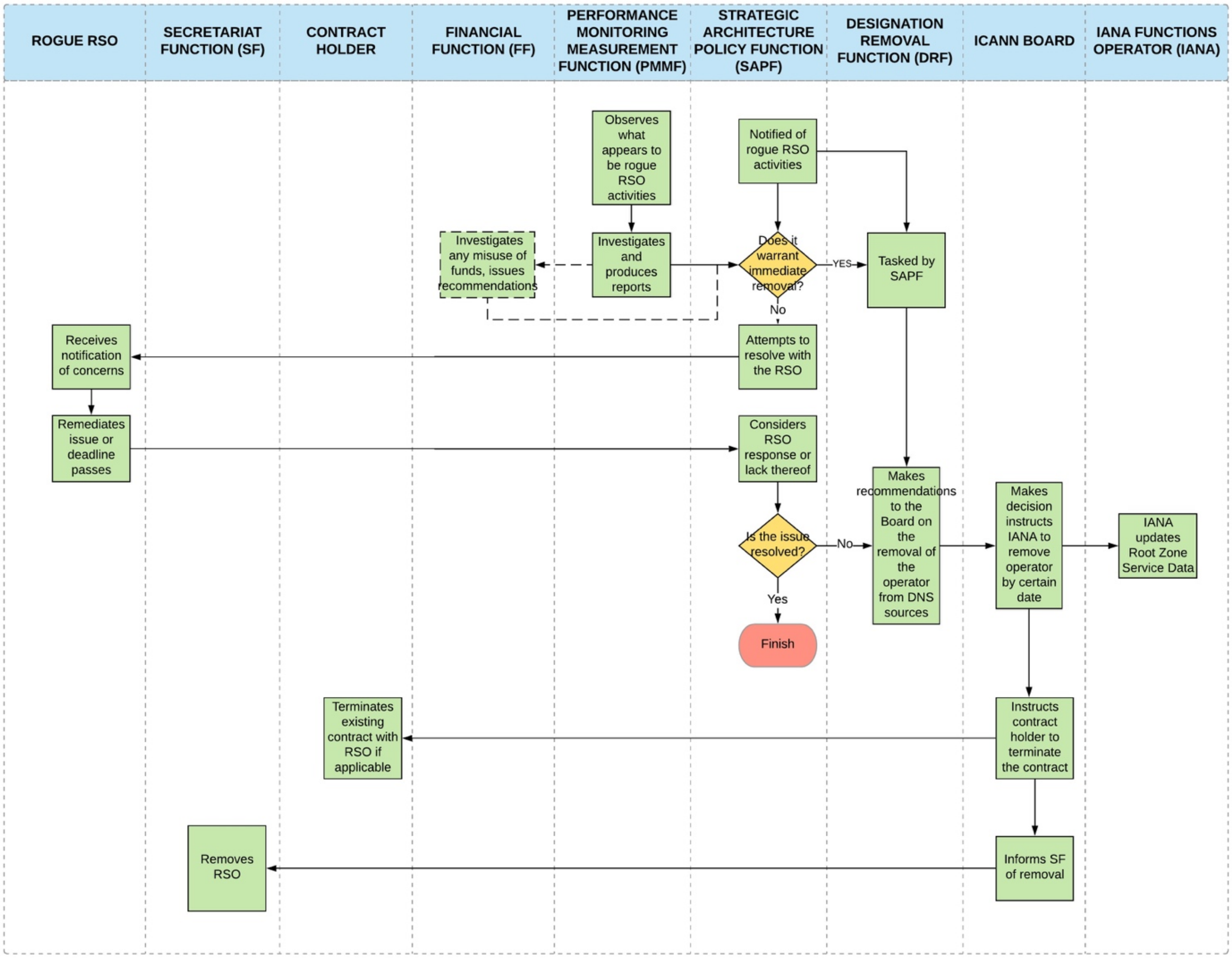
ROGUE RSO
SECRETARIAT FUNCTION (SF)
CONTRACT HOLDER
FINANCIAL FUNCTION (FF)
PERFORMANCE MONITORING MEASUREMENT FUNCTION (PMMF)
STRATEGIC ARCHITECTURE POLICY FUNCTION (SAPF)
DESIGNATION REMOVAL FUNCTION (DRF)
ICANN BOARD
IANA FUNCTIONS OPERATOR (IANA)
Observes what appears to be rogue RSO activities
Notified of rogue RSO activities
Investigates any misuse of funds, issues recommendations
Investigates and produces reports
Does it warrant immediate removal?
YES
Tasked by SAPF
No
Receives notification of concerns
Attempts to resolve with the RSO
Remediates issue or deadline passes
Considers RSO response or lack thereof
Makes recommendations to the Board on the removal of the operator from DNS sources
Makes decision instructs IANA to remove operator by certain date
IANA updates Root Zone Service Data
Is the issue resolved?
No
Yes
Finish
Terminates existing contract with RSO if applicable
Instructs contract holder to terminate the contract
Removes RSO
Informs SF of removal

Figure 8: RSO Goes Rogue Scenario

7. Conclusion

In their operations of the RSS, the 12 current RSOs have served the global community well. However, for the service to be sustainable, it is time for the operation and governance model to evolve. The RSSAC considers the Model to be a starting point that will require further deliberation, thoughtful analysis, and input from a broader set of experts from the ICANN community and beyond. The design of the Model assumes the current model of DNS root service delivery. The RSSAC recognizes that technologies evolve, including DNS technologies.

The RSSAC is committed to being a strong partner in further iterating and implementing the final version of the Model based upon the cornerstones of accountability, transparency, sustainability, service integrity, and resilience.

8. Acknowledgments, Dissents, and Withdrawals

The RSSAC would like to thank the following root server operators and their representatives for their time, contributions, and review in producing this publication.

Root Server Operators
Cogent Communications
ICANN
Internet Systems Consortium
NASA
Netnod
Réseaux IP Européens Network Coordination Centre
University of Maryland
University of Southern California, Information Sciences Institute
U.S. Department of Defense Network Information Center
U.S. Army Research Laboratory
Verisign, Inc.
WIDE Project and Japan Registry Services

Organizations with Liaisons to the RSSAC
Internet Architecture Board
IANA Functions Operator, ICANN
ICANN Security and Stability Advisory Committee
Root Zone Maintainer, Verisign

ICANN Support Staff
Mario Aleman
Kim Enger
Andrew McConachie (editor)
Carlos Reyes

Kathy Schnitt
Steve Sheng

This work started when the ICANN Board was under the leadership of Chair Steve Crocker. During that period, the ICANN Board recognized the importance of the effort that RSSAC had embarked upon and expressed its support. Under the leadership of Chair Cherine Chalaby, strong engagement from the ICANN Board continues. The RSSAC extends its appreciation and thanks to the ICANN Board for this level of support.

The RSSAC would also like to thank ICANN, University of Maryland, and Verisign, Inc. for their support hosting the six workshops where this publication was developed.

Workshop 1 | 23-24 September 2015
Planning Committee: Wes Hardaker, Daniel Karrenberg, Lars-Johan Liman, Kaveh Ranjbar, Tripti Sinha, Brad Verd

Workshop 2 | 11-12 May 2016
Planning Committee: Kevin Jones, Daniel Migault, Tripti Sinha, Brad Verd, Paul Vixie, Suzanne Woolf

Workshop 3 | 11-13 October 2016
Planning Committee: John Crain, Russ Mundy, Tripti Sinha, Brad Verd

Workshop 4 | 2-4 May 2017
Planning Committee: Tripti Sinha, Brad Verd, Suzanne Woolf

Workshop 5 | 10-12 October 2017
Planning Committee: Kaveh Ranjbar, Tripti Sinha, Brad Verd

Workshop 6 | 1-3 May 2018
Planning Committee: Kaveh Ranjbar, Tripti Sinha, Brad Verd

Dissents

There were no dissents.

Withdrawals

There were no withdrawals.

9. Revision History

9.1 Version 1

Current version.

Appendix A: Glossary of Terms

The following terms used in this document are taken from the RSSAC Lexicon version 1.[27]

instance. When anycast routing is used to allow more than one server to have the same IP address, each one of those servers is commonly referred to as an instance. For root servers, one refers to "an instance of J-Root" to mean one of the network locations answering to J-Root's IP address.

root server. The name of an entry point (instance) to the Root Server System cloud. Within the DNS technical community, a root server is a particular anycast instance, i.e. an authoritative name server that answers queries for the contents of the root zone.

root server operator. An organization responsible for managing the root service on IP addresses specified in the root zone and the root hints file.

Root Server System. The set of root servers that collectively implement the root service.

root service. The collective services provided by all anycast instances managed by all root server operators. These instances respond to DNS queries about the root zone. It does not matter which instance responds to a query. All root servers serving the same version/edition of the zone provide equivalent answers.

root zone (also called DNS root). In the DNS hierarchy, the zone that has no parent, as it stands at the top of the DNS hierarchy (inverted tree). The root zone contains all information needed to find top-level domains. Each edition of the root zone has a unique serial number and every root server is expected to have (and serve queries about) the current edition of the root zone.

Root Zone Administrator. The entity that manages the data contained within the root zone, which involves assigning the operators of top-level domains, such as .uk and .com, and maintaining their technical and administrative details.

Root Zone Maintainer. The entity responsible for accepting service data from the Root Zone Administrator, formatting it into zone file format, cryptographically signing it using the zone signing key (ZSK) for the root zone, and putting it into the root zone distribution system.

[27] See "RSSAC026: RSSAC Lexicon."

Appendix B. References

B.1 RSSAC Publications

“RSSAC001: Service Expectations of Root Servers,” 4 December 2015, https://www.icann.org/en/system/files/files/rssac-001-root-service-expectations-04dec15-en.pdf

“RSSAC016: RSSAC Workshop 2015 Report,” 7 January 2016, https://www.icann.org/en/system/files/files/rssac-workshop-07jan16-en.pdf

“RSSAC020: RSSAC Statement on the Client Side Reliability of Root DNS Data,” 28 June 2016, https://www.icann.org/en/system/files/files/rssac-client-reliability-root-dns-28jun16-en.pdf

“RSSAC023: History of Root Server System,” 4 November 2016, https://www.icann.org/en/system/files/files/rssac-023-04nov16-en.pdf

“RSSAC024: Key Technical Elements of Potential Root Operators,” 4 November 2016, https://www.icann.org/en/system/files/files/rssac-024-04nov16-en.pdf

“RSSAC027: May 2017 Workshop Report,” 16 June 2017, https://www.icann.org/en/system/files/files/rssac-027-16jun17-en.pdf

“RSSAC026: RSSAC Lexicon,” 14 March 2017, https://www.icann.org/en/system/files/files/rssac-026-14mar17-en.pdf

“RSSAC030: RSSAC Statement on Entries in DNS Root Sources,” 4 November 2017, https://www.icann.org/en/system/files/files/rssac-030-04nov17-en.pdf

B.2 RFCs

“RFC 2026: The Internet Standards Process – Revision 3,” October 1996, https://www.ietf.org/rfc/rfc2026.txt

“RFC 2418: IETF Working Group Guidelines and Procedures,” September 1998, https://tools.ietf.org/html/rfc2418

“RFC 2826: IAB Technical Comment on the Unique DNS Root,” May 2000, https://www.rfc-editor.org/rfc/rfc2826.txt

“RFC 7720: DNS Root Name Service Protocol and Deployment Requirements,” December 2015, https://tools.ietf.org/html/rfc7720