Root Zone Update Process Study

JAS ICJ

INITIAL REPORT – for public comment

18 January 2022

RESPECTFULLY SUBMITTED IN RESPONSE TO THE:
Request for Proposal for Root Zone Update Process Study
By: ICANN

submitted by:
an International Consortium led by JAS Global Advisors (ICJ)
Dr. Carolina Aguerre, Buenos Aires, Argentina
Dr. Joanna Kulesza, Lodz, Poland
Muriuki Mureithi, Nairobi, Kenya
Kurt Pritz, Thousand Oaks, CA, U.S.
Li Rui (Raymond), Beijing, China
Jeff Schmidt, Chicago, IL, U.S.

MANAGEMENT SUMMARY

The headlines of the Root Zone Update Process study are:

First, that IANA customers are delighted with the level of service that they receive from IANA. They are pleased both in their use of the Root Zone Management (RZM) System and in their personal interactions with IANA staff. Through the surveys and interviews conducted in this study, IANA customers recommended a relatively small number of improvements to the system and process. The IANA customers characterised these as "tweaks" to a well-operated, smoothly running process and should not be taken as anything but constructive improvements to a collegial, professionally managed organization.

Second, that the RZM study team found no single points of failure or unjustified redundancies. The findings of the IANA RZM process, systems and architecture study revealed a robust operation that is largely "right sized" given load, function, and resiliency requirements. The study's recommendations for improving security and efficiency resulted from the ICJ team investigations and, to a great extent, mirrored IANA's customer recommendations that were made in response to the survey and interviews with TLD managers. These recommendations were of no surprise to the IANA team, who have been contemplating how to make similar improvements while maintaining an open, accessible RZM change process.

A few examples are instructive:

Several survey respondents suggested that RZM system access should be protected by multifactor authentication, like those routinely employed in many online accessed systems. However, there are counterbalancing considerations, which are discussed in the body of this study. ICJ does not believe requiring the use of multifactor authentication will materially improve the security of the system when viewed in its entirety, but we do make recommendations for improving the security of IANA-TLD Manager communications via the RZM system.

During the survey, it was found that some TLD contacts were not reachable for a variety of reasons; e.g., designated contacts sometimes use personal, rather than role, email addresses and contact is lost when they move on to other jobs. Another study has confirmed this "reachability" issue. Unreachability could present a stability / security issue in the event of an emergency. IANA should take a set of recommended steps to improve reachability.

In addition, several respondents indicated that nameserver Tech Checks often unnecessarily delayed the change request process and recommended changes in the approach to Tech Checks that might improve their efficiency and efficacy.

RZM Study Methodology: In accordance with the RFP requirements, this study was accomplished in three parallel tracks:

- Systems, software architecture, and Security, Stability, Resiliency (SSR) review
- Process management review
- Communications and stakeholder reviews accomplished through a survey and interviews.

Every TLD manager was sent a survey. We received 90 responses representing between 700 and 900 TLDs (depending on how the timing of industry consolidations are considered).

While the three tracks performed work in parallel, the work plan made provision for collaboration and sharing of results among tracks. In this way, the customer perspective of the process flows and security measures could be compared to that determined by the ICJ team's analysis of IANA practices and documentation. These sorts of feedback loops provided a type of verification for the report's conclusions. This worked out better than hoped as the results of surveys and interviews were fed back to the IANA team and the IANA reactions were then considered by IANA's customers.

This report includes a separate section on each of the three tracks. That is followed by a set of Issue Discussions that integrates the results of the three tracks and describes specific findings and recommendations. These recommendations are a jumping-off point for a collaboration among IANA and its customers to consider changes to the RZM change request process.

INTRODUCTION

Background

Historically, the U.S. Department of Commerce (DoC) played an active role in the coordination and management of the DNS. After a nearly two-decades long process that culminated on 1 October 2016, the DoC's role was transitioned to the private sector as part of an effort called the IANA Stewardship Transition. As part of the planning for this transition, the IANA Stewardship Transition Coordination Group (ICG) released a document in March 2016 entitled "Proposal to Transition the Stewardship of the Internet Assigned Numbers Authority (IANA) Functions from the U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA) to the Global Multistakeholder Community." This document[1] proposed a plan to implement the transition and included additional recommendations, including a call for a "formal study" to be conducted to examine the operational procedures governing changes to the root zone after the NTIA's involvement ceased.[2] This is that study.

Study Objectives

The objectives of this study are to investigate whether there is a need to increase (and if so, how) the robustness of the operational arrangements for making changes to the root zone content, identifying any single points of failure that may exist and, should they exist, offering recommendations on how to reduce or eliminate them.[3]

The scope of the study is the processing of change requests to the DNS root zone. This process typically begins with a TLD manager's request for a change and ends with the publication of a new root zone on the Root Zone Maintainer's platform for distributing the root zone to the Root Server Operators (RSOs).

This includes:

- the process and means by which a TLD manager submits a root zone change request to the IANA[4],
- all policies in place, tasks performed, and systems used by IANA to evaluate and process a requested root zone change, from receipt of the request from the TLD manager through the means and mechanism by which the change request is communicated to the Root Zone Maintainer,
- all communications between IANA and the Root Zone Maintainer, and
- all policies in place, tasks performed, and systems used by the Root Zone Maintainer to evaluate and process a requested root zone change, from receipt of the request from IANA through the means and mechanism by which the signed root zone is distributed to the Root Server Operators.

The scope instructed the study provider to look for opportunities to improve the overall architecture and process along several dimensions:

- Efficiency: Are there unnecessary steps or complexity?
- Robustness: Are there single points of failure?
- Conformance: Does the process ensure that the intended root zone changes are made following the policies established by the ICANN community?
- Confidentiality: Do communications between various parties meet the level of confidentiality required by the system?

[1] https://www.icann.org/en/system/files/files/iana-stewardship-transition-proposal-10mar16-en.pdf

[2] https://www.icann.org/en/announcements/details/request-for-proposal-for-root-zone-update-process-study-28-4-2020-en

[3] https://www.icann.org/en/announcements/details/request-for-proposal-for-root-zone-update-process-study-28-4-2020-en

[4] I.e., the IANA Naming Functions as conducted by PTI under contract from ICANN or similar

- Integrity: Does the system ensure the integrity of data, both in transit among various parties and at rest?
- Availability: Do the system's components meet the appropriate availability requirements?
- Transparency: Is the operation of the system sufficiently transparent and auditable?

The Work Plan & Report Layout

To comply with the RFP requirements, a work plan was developed and comprised of three tracks:

- Systems, software architecture, and Security, Stability, Resiliency (SSR): to ensure that IANA processes are secure, stable, and resilient to accidental or malicious changes,
- Process management: to ensure that IANA processes are necessary and sufficient, efficient, effective, and resilient, and
- Communications and Stakeholder consultation: to ensure that every IANA customer everywhere in the world receives and recognizes the same high level of support delivered efficiently and effectively.

While the three tracks performed the work in parallel, the work plan made space for collaboration and sharing of results so, for example, that the IANA view of the process flows were compared to the customer perspective, and also that the security measures specified in documentation were an actual part of the process flows.

Each of the three tracks resulted in a separate section of this report:

- detailing the methodology, and
- reporting the findings.

In cases where the finding indicated that changes in the process, systems or architecture should be considered, those discussions were separated into Issue Discussions under the report heading: Findings, Recommendations and Rationale.

These Issue Discussions include:

- recommended changes (if any) to the process, systems, or architecture,
- identification of single points of failure (if any), and
- a rationale and cost-benefit analysis using information developed during information exchanges with IANA staff, IANA customers, and the Root Zone Maintainer.

During the drafting process, the ICJ team and IANA teams met to fact-check the findings – not to edit outcomes or recommendations, only to make sure all agreed on the fact sets that support them.

The Team

The International Consortium led by JAS Global Advisors (ICJ) was specially formed for this effort and its requirements. ICJ's diversity spans several dimensions: experiential, cultural, geographical, educational, and technical. The team is comprised of individuals well-known to the DNS and security communities, and whose work and judgment have been rightfully trusted after building a reputation for integrity.

JAS Global Advisors brings extensive technical familiarity with the Internet DNS, IANA, and ICANN ecosystem and counts global financial institutions, government agencies, and critical infrastructure providers as valued clients.

ICJ team members have:

- experience developing, managing, and measuring operational processes for major corporations with high security, strict deadlines, and cost constraints,
- experience covering every level of the DNS and domain name industry: as registrants, internet governance experts, TLD operators, DNS security advisors to the highest corporate and governmental levels, and NIC operators,
- an understanding of the technical, procedural, and political environments in which IANA operates, and
- the ability to communicate with IANA's customers with in-region experts who understand unique local issues and varying approaches to risk tolerance, communication, security, and the varying political environments.

CUSTOMER COMMUNICATION TRACK

IANA Principle: Ensure that every IANA customer everywhere in the world receives and recognizes the same high level of support delivered efficiently and effectively

Methodology

To gain a complete understanding of IANA's processes and systems, we sought the knowledge and advice from IANA's customers, i.e., TLD managers, who have been interacting with IANA for many years. With that goal in mind, we developed a survey that was made available to all TLD managers and, depending on the responses received, selected several TLD managers for follow-up interviews. The interviews provided the opportunity for a "deeper dive" into the issues identified in the surveys and the result is a set of recommendations based on IANA customer requirements.

The design and execution of the survey was guided by the following principles and objectives:

1. The primary purpose of receiving the input of IANA customers is to ensure that IANA objectives, priorities, security measures and process steps match the needs and expectations of their customers. Disparities in expectations or perceptions might indicate areas for improvement, cost saving or process changes.

2. The ICJ team included DNS professionals in each of the ICANN regions to effectively communicate on the same professional and cultural level and better relate the business values, risk tolerances, communications tendencies, approaches to security, and the political environment on a regional level.

3. To reach all IANA customers, a voluntary survey was designed to identify TLDs that either have or might have applied to make a root zone change since the IANA separation. Survey responses were used to determine their experiences and which TLD managers should be interviewed by in-region team members.

4. Surveys and the subsequent interview questions were based on the requirements described in the ICANN RFP, the joint DNS and regional experiences of the team, the responses from the surveys, and from the process flows generated during the interviews with IANA. The questions sought to discover if IANA and their customers have the same sense of:

   a. which, if any, additional process steps are needed,

   b. which, if any, process steps are unnecessary,

   c. what economies might be realized,

   d. what avoidable burdens are imposed during the root zone change management process,

   e. which security improvements are necessary, and

   f. which security measures are unnecessary.

5. The ICJ team compiled the responses into a set of findings, tested those findings through interviews with IANA staff and follow-ups with TLD managers, and synthesized those findings with the other work streams to develop a tentative set of recommendations.

Survey Execution & Results

The survey was designed with three goals in mind, to: (1) encourage participation; (2) create an easy-to-use opportunity for TLD managers to provide meaningful feedback; and (3) assist in answering the RFP-posed questions described above.

To encourage participation, the ICJ team sent an advance email to each TLD manager (the Administrative Contact) explaining the study, the purpose of the survey, and the singular opportunity this study presents. In addition, the survey (included in full in the appendix) was designed to be completed in under ten minutes. All questions had clearly delineated multiple-choice components. Finally, the advance email offered TLD managers the opportunity to receive a translated version of the survey into whichever language they preferred. As a result, TLD managers completed 85 surveys in English, four in Spanish, and one in Russian.

To create the opportunity for TLD Managers to provide meaningful feedback, many questions allowed for open-ended responses. This enabled the respondent to raise issues easily and in their own words, as opposed to trying to identify issues through additional multiple-choice questions. For example, when one question sought to identify if there were any perceived security issues, the affirmatively answering respondent was simply asked, “tell us about it,” rather than being presented with a list of possible security issues that might or might not match the respondent’s concern.

In addition, the IANA team reviewed the surveys prior to their distribution and requested two questions be added:

1. Does the English-language requirement in the provision of the RZM change process present a significant obstacle to the timely and repeatable provision of those services (and to what extent is there a preference for operation in a language other than English)?

2. To discover whether TLD managers were aware that IANA offers and provides a heightened level of support and guidance (a “white glove” service) to TLD managers making a complex set of change requests.

In requesting these questions, the IANA staff constructively sought to leverage the survey opportunity with the intention of improving services if a need was identified.

To answer the RFP-posed questions, the survey questions were mapped to the RFP delineated objectives listed in paragraph (4) above. To gain a full understanding of the issues being raised by the respondents, a comment box or open-ended question was made available whenever a respondent raised an issue. This gave the respondent a chance to answer the question in her / his own words. In addition, where issues raised by responses were not clear to the ICJ team, interviews were scheduled so that full, clear feedback could be obtained.

Survey Responses

This report includes summarized and raw data. This section summarises the survey responses. All survey responses can be found in the appendix (in anonymized form).

We received 90 responses that represented 721 (and as many as 900) TLDs. (That last number is described as a range as it is dependent on how the reader considers the TLD consolidations and mergers that were occurring as the time the survey was being conducted.)

a. *Surveys sent*

A survey was sent to every TLD manager using the IANA Root Zone Database (see, https://www.iana.org/domains/root/db). The Administrative contact addresses were used. To reduce the number of duplicative emails, only one email was sent in cases where TLDs shared the same email or physical address. Therefore, the number of surveys sent were significantly fewer than the number of TLDs in the root zone.

Africa region:	59 survey invitations (54 ccTLDs, 5 gTLDs)
Asia-Pacific region:	145 survey invitations sent (85 ccTLDs, 73 gTLDs)
Europe region:	251 invitations sent (74 ccTLDs, 177 gTLDs),
Latin America region:	49 invitations sent (37 ccTLDs, 12 gTLDs)
North America region:	107 invitations sent, (8 ccTLDs, 99 gTLDs)

Interestingly, 29 of the emails “bounced” as the email address in the Root Zone database were not functioning for some reason (e.g., “mailbox full,” “no such user,” or the recipients email system refused to make or accept a connection). This lack of “reachability” has been identified as an issue in other fora.

As an example, some TLD managers choose to provide an individual’s email, as opposed to a role email, and this may be a disadvantage. We found several variations of this issue reported:

- The person left the organization and left no one in charge of their IANA account.
- The person moved to a different department and was filtering out emails pertaining to these requests.
- The company changed email platforms and did not forward role emails from the old address to the new one.
- Contacts use their personal email rather than work email, (person.someone@gmail.com) vs (person.someone@theircompany.com).

Recognizing this as a potential SSR issue, some respondents suggested that a “role contact” be appointed with the raison d’être of responding to IANA contact attempts. Others recommended regular audits to ensure contacts are kept up to date and accurate.

This is less of a problem (and therefore less of an SSR issue) for IANA as they can make use of private email lists that IANA otherwise uses to make contact regarding operational issues. Additionally, IANA occasionally leverages the Governmental Advisory Committee (GAC) to identify contacts in specific regions responsible for ccTLDs.

The “reachability” issue is described in detail in the Issue Discussions section below.

b. *Survey responses received*

90 survey responses received, 1 in Russian, 4 in Spanish, 85 in English.

gTLD operators (incl. ‘portfolio’ operators):	28
ccTLD operators in Africa region:	7
ccTLD operators in Asia-Pacific region:	9
ccTLD operators in Europe region:	29
ccTLD operators in Latin America region:	16
ccTLD operators in North America region:	1

The 90 survey respondents represented 721 TLDs in total (with consolidations occurring around the time of the survey making that number close to 900). Surveys were received during the period 7-30 April 2021.

There was information to be derived from those who did not respond to the survey. For example, the team noted that some TLDs that had not responded also had not made a root zone change request in a relatively long time. Reaching out to certain TLDs that did not respond to the survey led to findings described in subsequent sections of this report.

The average time to complete the survey was 8 minutes 51 seconds.

Survey Findings

The survey responses led to conclusions that are described below. In certain cases, those conclusions were tested in follow-up interviews, in discussions with the IANA team, and by reaching out to certain TLD managers that did not respond to the survey.

The survey's conclusions:

1. Those that "rarely or never" use the IANA change management process do so because their TLD is stable in its operation (i.e., rarely changing personnel or infrastructure), and not because they find the process difficult or onerous.

   Nearly half of the respondents (49%) use the IANA RZM function 1-2 times per year- the generally accepted average usage. Of those that used IANA services less frequently, 100% of responses who responded "rarely or never" said it is because their operation is stable (questions 2 and 3).

   (In one instance there was outreach to a TLD manager who did not respond to the survey. That TLD manager stated that: the RZM change process was too "stringent" and only undertook changes when absolutely necessary. Contact information for this single example was reported to IANA separately.)

2. As a point of interest, recent RZM change requests by TLD managers where:

   a. 84% requested technical re-configuration of domains, i.e., changes to nameservers and DS records,

   b. 64% requested changes to points of contact for TLDs,

   c. 33% requested other items (e.g., WHOIS, RDAP), and

   d. 22% requested transfers to a new TLD manager, i.e., a change of control.

3. IANA customers are unqualifiedly satisfied with IANA response times.

   a. 90% stated that the time to complete the RZM process is "about right,"

   b. 6% stated "too long," and

   c. 4% stated "too quick."

      Looking into the "too long" responses and comparing those responses to the IANA published processing steps, we found that reductions in response times are not feasible without removing necessary safeguards from the process.

The next two bullet points result from responses to the two survey questions after the one above provided additional evidence of high levels of customer satisfaction. In several instances, respondents followed their positive feedback with suggestions (in open-ended questions) for certain improvements. Without exception, these TLD managers explicitly stated that, by making these suggestions, they were seeking to make an excellently managed RZM process better and were in no way attempting to qualify their earlier attestations to the excellence of the process and customer service levels.

4. 96% of the responses stated that there were no unnecessary steps or procedures in the RZM change process. However, the open-ended commentary to this question caused additional examination into the "Tech Check" process whereby IANA checks nameserver configuration (according to published criteria) prior to processing nameserver and DS change requests.

   Two specific Tech Check issues were raised in the survey and follow-up interviews: serial number synchronization, and the use of the "double DS" method to roll KSK. These issues are addressed in the Technical Checks Issue Discussion.

5. RZM system users generally agree there are no costly or burdensome steps to the process (92% of respondents indicated there are none), reflecting a high level of satisfaction. Respondents raised one process that unnecessarily imposed a time burden, known as the "glue policy."

   This situation arises where one TLD is served by a name server that is authoritative for several TLDs. When one TLD wishes to make a name server change, the backend provider (and IANA) must get approval for the change from all other TLDs sharing this authoritative server. This practice may slow and generally frustrate the RZM process.

   In our discussions with the IANA team, we learned that the next version of the RZM system addresses this issue, switching it from an "endorsement" model to an 'objection' model. When this is implemented, when there is a "glue" change, one other TLD must affirmatively approve the change and there will be a seven-day objection window for other TLDs sharing that authoritative server to reject the change.

   One other issue surfaced regarding efficiencies that might be easily realised. The language IANA uses while reporting exceptions when waiting for a response from a TLD contact is ambiguous as to which specific contact has not responded. More detailed information would speed the customer's corrective action steps. The IANA staff reviewed and agreed with this assessment.

The next two points were a result of questions inserted at IANA staff request, who constructively sought to leverage the survey to identify possible improvements to their services.

6. IANA provides a "white glove" service to aid in the handling and processing of complex requests and sought to find if TLD managers were aware of it and were predisposed to use it.

   a. 67% of respondents stated that additional help was not needed

   b. 28% were not aware of the availability of supplementary advisory and coordination services

   c. 6% had made use of it.

   The answers indicate an opportunity to make more TLD managers aware about the benefits of the service.

7. IANA also sought to determine if providing service in languages other than in English was necessary or desirable. While gTLD contracts (and an understanding with ccTLDs) require that all TLD managers be able to communicate in English with IANA, IANA sought to determine if servicing non-native English speakers in their native languages would improve customer comfort or efficiency.

   Of the 90 responses, ***none*** called English a significant obstacle to its application for Root Zone Management changes. However, 17 TLD managers stated a preference to work in another language. Of those that went on to state a preference:

   a. Seven requested Spanish

   b. Two requested French

   c. One requested Chinese

   d. One requested Portuguese

The question of whether to make language services available is complex, with cost-benefit and communication ramifications. We don't recommend the immediate implementation of language services and discuss the issue and provide guidance in the Issue Discussion section below.

8. While 82% of survey respondents do not believe there are vulnerabilities and that the security measures in the RZM change process are sufficient, 18% described potential weaknesses. In the open-ended portion of the survey questions, these respondents indicated that IANA should employ multifactor authentication to use the RZM System. These comments were discussed during the subsequent interviews.

   As part of the study, we were able to discuss these responses with the IANA team. Aside from the unique practical challenges, a tenet of the RZM process is that it is open to anyone to submit requests, not just designated contacts (e.g., accounts with authentication established). This principle obviates the implementation of blanket multifactor authentication or even a requirement for an established user account.

   This topic is discussed in the Issue Discussion section below.

9. Like the point above, 92% of the respondents indicated there were no weak or single points of failure in the RZM system. Most comments for this question address the same issues as for the question described just above. Multiple comments also raised the use of email as a primary communication tool (rather than a web application) and the risks arising out of the possibility that an email address might be subject to a business email compromise ("BEC").

   Given that the RZM is a process open to all, some email communication is necessary. However, IANA staff recognize the risks inherent in the use of email, provides safeguards to address the risks, and will continue discussions with their customers to minimize the risk by considering additional communications mechanisms.

10. Overwhelmingly respondents confirmed that the RZM process works smoothly and efficiently and reiterated positive feedback when asked about the effects of IANA independence from the USG. Significantly, all respondents stated that, since the separation: (1) IANA performance was fine then and is equally fine now, or (2) that IANA service was fine then and continues to improve.

PROCESS MANAGEMENT TRACK

Methodology

IANA Principle: IANA processes are necessary and sufficient, efficient, effective, and resilient.

1. The ICJ team followed a classical process management approach where we created process flowcharts of the entire root zone management change request process and determined the value added by each step to determine whether the process can be streamlined. A corresponding risk analysis determined whether additional steps in the process were required. Finally, we considered the potential cost of making changes.

2. A single-point-of-failure analysis was conducted during the process flow analysis, again in a classical way, by eliminating access to resources used in each step and determining if that step (or the IANA change management process as a whole) is recoverable in a way that it can operate within current SLAs.

3. If it was determined that a process step could fail with no effect on completion of the IANA task, that would raise a presumption that the step is not necessary: with that presumption to be tested with customers and other stakeholders.

4. The flowcharts were derived from two sources: IANA policies and procedures, and interviews with IANA team members as they took the ICJ team through different root zone management processes, sub-processes, and scenarios. Discrepancies between the documentation-based flows and the interview-derived flows were discussed and reconciled during this process.

5. Process flows were developed to accommodate the different types of root zone management changes, e.g., change of control (i.e., re-delegations), Admin or Tech Contact changes, nameserver changes, emergency change requests, and gTLD retirement.

6. In anticipation of the cost-benefit analysis to follow the recommendation of any potential changes, we sought to understand: the cost / effort of each process step, the administrative cost of making procedural changes to a process step, the risks associated with eliminating a step, and the benefits of (or reasons for having) that step.

7. In the steps described above, we sought to demonstrate (or not) that the IANA processes are robust and economical, and that each step in the process is both necessary and sufficient.

8. Then (using the results from the Communications track), we compared the process flows generated in this track with the expectations of IANA customers to see if their understanding of the processes match, as well as customer thoughts on the value of each step.

The manner in which this plan was executed:

1. The ICJ team requested and received process documentation from IANA. These included flow diagrams and written descriptions of each step, the actor responsible, a link to relevant documents and actions. Examples of this documentation can be found in the appendix.

2. Using that documentation, we constructed process flows and listed questions where we found the documentation furnished to be incomplete, vague, or potentially contradictory.

3. We met with the IANA staff (remotely) in a set of three, two-hour sessions where we reviewed each of the IANA processes and subprocesses in detail, sought answers to our questions, and discussed some of the issues raised by IANA's customers through their participation in the survey and interviews.

4. Email exchanges resolved outstanding questions.

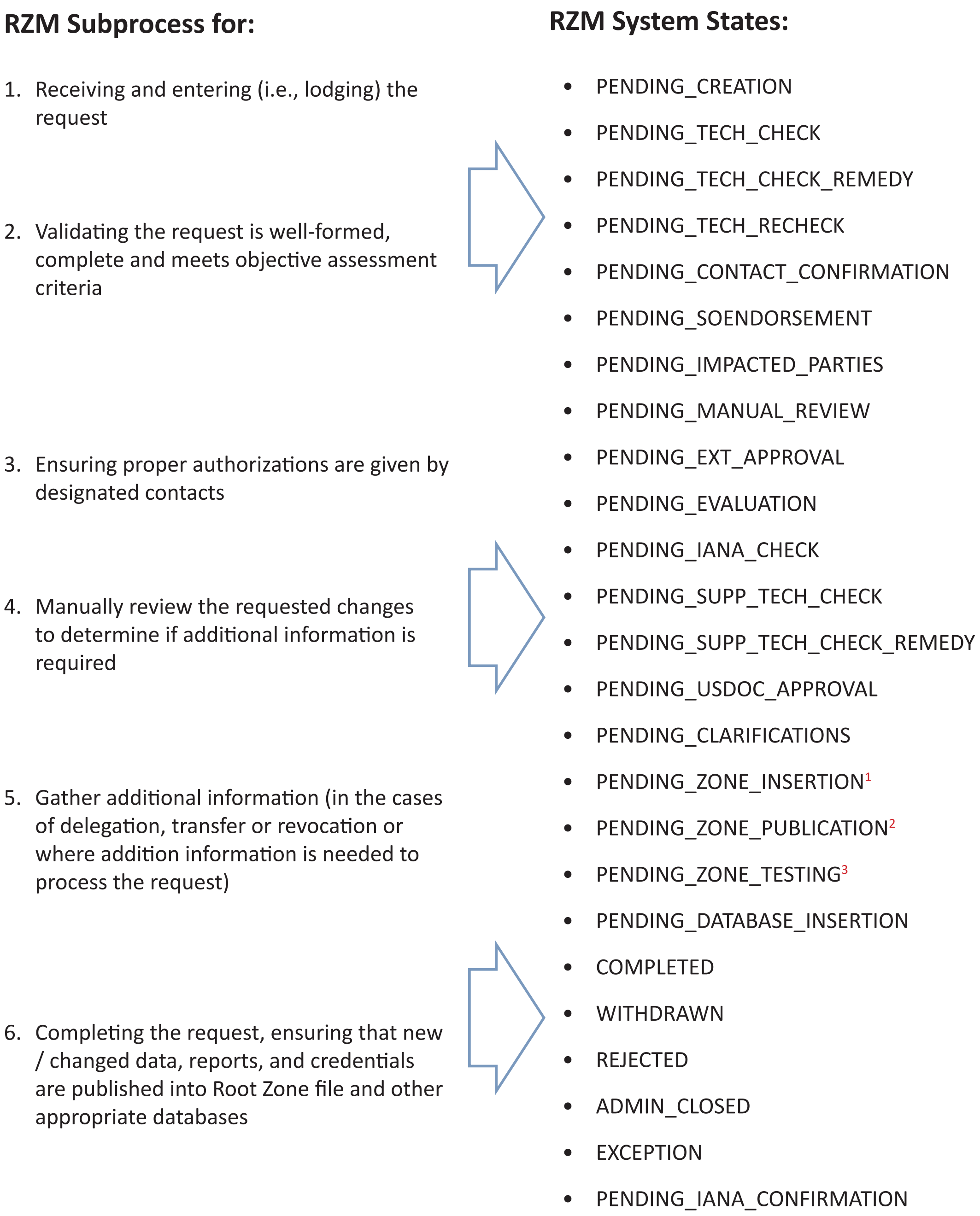
Results and Findings

IANA operates a unified Root Zone Management Change Request process that is employed for all routine root zone management change requests and is comprised of six sub-processes:

- The sub-process for receiving and entering (i.e., lodging) the request
- The sub-process of validating the request is well-formed, complete and meets objective assessment criteria (including "Tech Check")
- The sub-process of ensuring proper authorizations are given by designated contacts
- The sub-process to manually review the requested changes to determine if additional information is required
- The sub-process to gather additional information (in the cases of delegation, transfer, or revocation or where addition information is needed to process the request)
- The sub-process that completes the request, ensuring that new / changed data, reports, and credentials are published into Root Zone file and other appropriate databases

Under the Root Zone Management Change Request process "umbrella," there are two specialized processes to address gTLD revocations and emergency changes. Both the gTLD Revocation Process and the Emergency Root Zone Change Process also use the same sub-processes.

The sub-process are informal divisions that pre-date the implementation of the Root Zone Management System (RZMS). The Root Zone Change Process and its sub-processes are comprised of (and can be more accurately described by the complete set of 'states' from the RZMS workflow). TLD Managers and other users of the RZMS will be familiar with these states.



RZM Subprocess for:

1. Receiving and entering (i.e., lodging) the request
2. Validating the request is well-formed, complete and meets objective assessment criteria
3. Ensuring proper authorizations are given by designated contacts
4. Manually review the requested changes to determine if additional information is required
5. Gather additional information (in the cases of delegation, transfer or revocation or where addition information is needed to process the request)
6. Completing the request, ensuring that new / changed data, reports, and credentials are published into Root Zone file and other appropriate databases

RZM System States:

- PENDING_CREATION
- PENDING_TECH_CHECK
- PENDING_TECH_CHECK_REMEDY
- PENDING_TECH_RECHECK
- PENDING_CONTACT_CONFIRMATION
- PENDING_SOENDORSEMENT
- PENDING_IMPACTED_PARTIES
- PENDING_MANUAL_REVIEW
- PENDING_EXT_APPROVAL
- PENDING_EVALUATION
- PENDING_IANA_CHECK
- PENDING_SUPP_TECH_CHECK
- PENDING_SUPP_TECH_CHECK_REMEDY
- PENDING_USDOC_APPROVAL
- PENDING_CLARIFICATIONS
- PENDING_ZONE_INSERTION[1]
- PENDING_ZONE_PUBLICATION[2]
- PENDING_ZONE_TESTING[3]
- PENDING_DATABASE_INSERTION
- COMPLETED
- WITHDRAWN
- REJECTED
- ADMIN_CLOSED
- EXCEPTION
- PENDING_IANA_CONFIRMATION

Among the RZM System States, the Root Zone Maintainer (Verisign) process has three components –

1. pending insertion (Verisign has received the request but hasn't approved it for publication),
2. pending publication (Verisign has accepted the change for publication; they have yet to issue a new zone file with it),
3. pending testing (Verisign indicates it is now published but we have yet to observe the change in the DNS)

Figure 1: The sub-process are informal divisions that pre-date RZMS and are comprised of the complete set of 'states' from the IANA RZMS workflow. Each state signifies a required action by IANA, an IANA customer, or (in three cases) the Root Zone Maintainer, Verisign. (The state requiring U.S. approval is now bypassed but is still in the system so is included here for completeness.)

As described above and to test our understanding, we used IANA documentation to create flowcharts describing the sub-process and to raise questions arising about the RZM process. (A list of documentation requests and a set of IANA provided documentation can be found in the appendix.)

In certain cases, our examination of the processes or our interactions with IANA customers raised issues suggesting changes to the process. For the cases where changes are recommended or requiring more in-depth discussion or analysis, we prepared a set of Issue Discussions that can be found in another section of this report. As a prerequisite to the Issue Discussions, we first describe each of the IANA processes and sub-processes, and the questions raised.

The Root Zone Management Change Process

The overall RZM change process can be described by its component subprocesses:

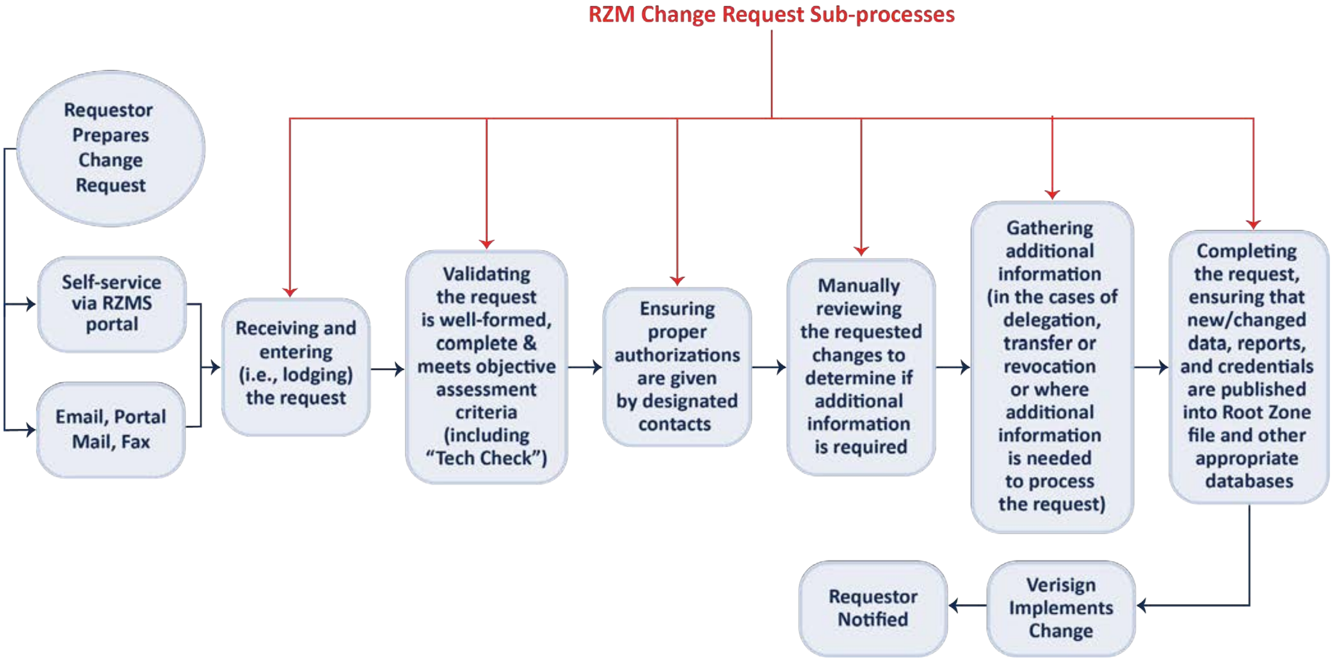

RZM Change Request Sub-processes
Requestor Prepares Change Request
Self-service via RZMS portal
Email, Portal Mail, Fax
Receiving and entering (i.e., lodging) the request
Validating the request is well-formed, complete & meets objective assessment criteria (including "Tech Check")
Ensuring proper authorizations are given by designated contacts
Manually reviewing the requested changes to determine if additional information is required
Gathering additional information (in the cases of delegation, transfer or revocation or where additional information is needed to process the request)
Completing the request, ensuring that new/changed data, reports, and credentials are published into Root Zone file and other appropriate databases
Verisign Implements Change
Requestor Notified

Figure 2: Root Zone Management Change Request Process indicating each of the IANA Change Request Sub-processes

Without getting into the details of each step (they will be addressed in the subsequent sub-process flows), the overall flow gave rise to certain questions.

1. Is the contact authorization equivalent to a "two or multi-factor authentication"?

   The possibility of adopting multi-factor authentication as a prerequisite to accessing the RZM System was raised by IANA customers during the survey and interviews. Reading the supporting documentation, the designated contact confirmation step seemed to address or partially address the issues raised by IANA customers. Through our discussions with the IANA team, we found that the contact confirmation step provided adequate protections against implementation of unwanted root zone changes, but we also came to understand potential security risks in the communications platforms used and possible improvements. These are discussed in the Issues Discussion section.

Taking the next two questions together:

2. Does this process apply to all types of change requests? Where are distinctions among request types made?

3. How is eligibility for changes of control (delegation / revocation / transfer) determined and to what types of requests does it apply?

   The IANA documentation describes one process flow for all routine change requests: e.g., changes of control, name server changes, contact changes. However, higher levels of scrutiny are required depending on the request type due to their varying effects on TLD stability and security (and also on whether a change can be reversed if necessary). Discussion of questions two and three above and an examination of IANA documentation provided an understanding that decision trees within each process and sub-process provide for heightened scrutiny when necessary. Therefore, having one IANA overall process does not add unnecessary steps for "simple" changes or open the door to risks for "complex" changes.

4. When does the Supplemental Tech Check apply?

   An issue raised by IANA Customers is the manner and timing in which Tech Checks are conducted. Their concerns are described more fully in the Customer Outreach section. Generally, the RZM System automatically determines whether a supplemental Tech Check is required. The supplemental technical check represents the technical checks being reperformed just prior to a request being transmitted to the Root Zone Maintainer. Repeating the tests is to check for situations where the configuration falls out of compliance during the time other processes steps are being conducted. This is particularly important for TLD delegation and transfer requests in which many months may have elapsed since the original request was submitted and the technical checks were first performed.

   As described in the Customer Outreach section and the Issue Discussion section, the Tech Check pass/fail criteria can lead to "false negatives" where configuration changes might not be registry operation failures. While this does not result in a security issue (at least directly), it can delay the RZM process and materially inconvenience customers. IANA, through consultations with its customers, has considered amendments to the Tech Check process that will be brought to the community for discussion. These are described in the Issue Discussion section on this topic.

5. At which points can requestors cure deficiencies?

   The answer to this question is essentially, "anytime." IANA customers average one to two requests per year so, from a customer standpoint, each change is a brand-new experience (i.e., not routine). This leads to missteps on the customers' part. The uncertainty or resulting delays might discourage customers from engaging in the process. To ameliorate that eventuality, IANA seeks to facilitate the request with repeated checks, where the customer is solicited for correction where required. The customer surveys and interviews indicated some areas where IANA requests for additional information could be clearer, e.g., in the area of contact information during administrative or technical contact changes. In a separate effort to help customers, IANA has implemented a "white glove" program to help customers with complex requests or where they have little / no experience with the RZM system.

We now examine each of the sub-processes that occur during the RZM Change process:

Receiving and Entering (i.e., Lodging) the Request

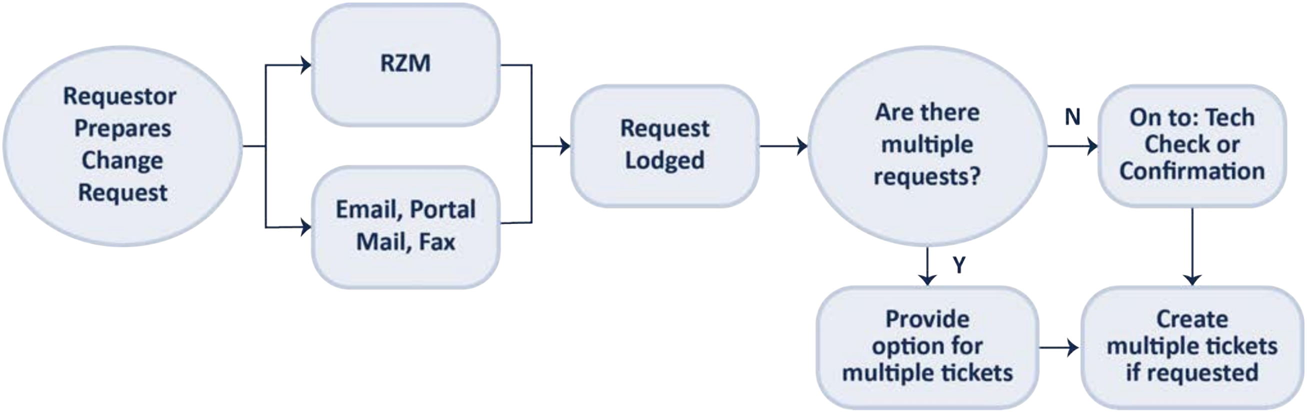

Requestor Prepares Change Request
RZM
Email, Portal Mail, Fax
Request Lodged
Are there multiple requests?
N
On to: Tech Check or Confirmation
Y
Provide option for multiple tickets
Create multiple tickets if requested

Figure 3: IANA Change Request Sub-process: Receiving and entering (i.e., lodging) the request

Flexibility for the benefit of the customer is a hallmark in this preliminary part of the process:

- Customers may request an RZM change using the RZM System or by email, post, or fax.
- Customers may request that multiple requests submitted be processed simultaneously or separately to expedite one or more.

Two questions were raised:

1. Are there criteria for measuring request completeness or adequacy?

   Request completeness is checked on a rudimentary basis at this stage of the process. Automated checks for what might be termed “wellformedness” are conducted. For example, fields that are mandatory are checked, and fields with certain expectations for format are validated, i.e., the keytag on a DS record must be an integer within bounds.

   If the request is deficient in some other manner, it is important to return to the customer in a timely manner with questions regarding those potential deficiencies. This examination occurs in the subsequent subprocess that begins essentially instantaneously upon receipt, right after the request is lodged.

   For those requests not made in the RZM system (e.g., via email), an IANA team member enters the request into the system. As is described later, the IANA process documentation does not include criteria for decision making as to the completeness of an application. In some cases, this criteria in built into the RZM system, and in other cases it is implicitly incorporated by the experience and knowledge of the IANA team members. Given this, we find no single points of failure based on the absence of these criteria from some of the decision points but, in the Issue Discussion covering this topic, we recommend that the process documentation be augmented to include these criteria.

2. Is the determination of whether Tech Check is required made at this point? By whom is the determination made?

   The RZM system automatically schedules Tech Checks for all nameserver and DS record changes.

Tech Check (Validating the Request is Well-formed, Complete & Meets Objective Assessment Criteria)

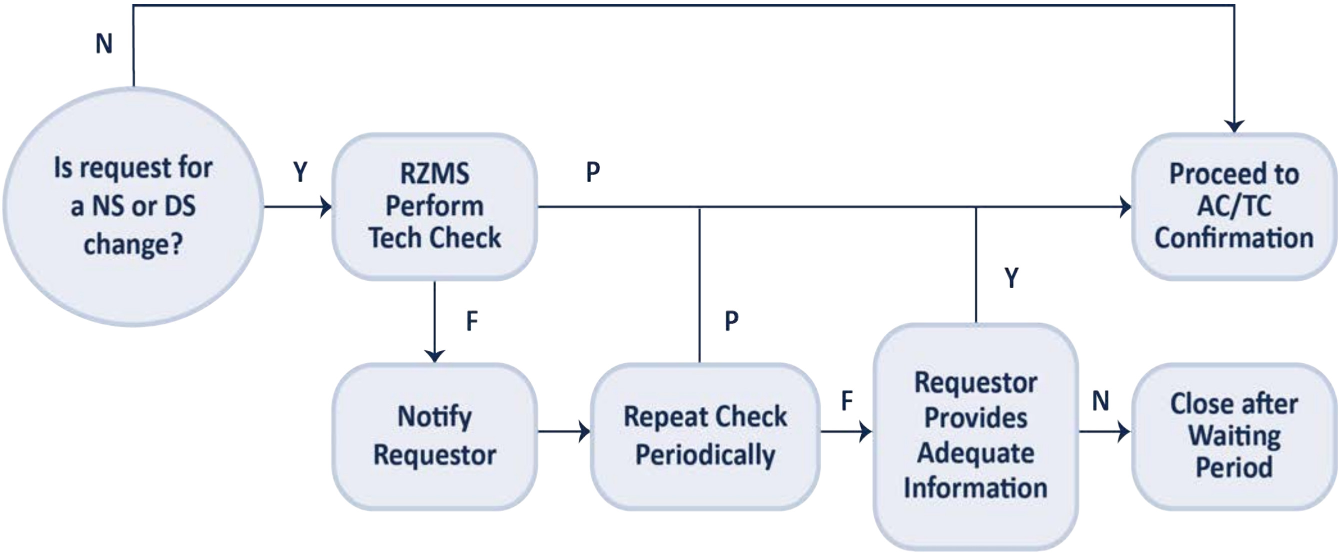

N
Is request for a NS or DS change?
Y
RZMS Perform Tech Check
P
Proceed to AC/TC Confirmation
F
P
Y
Notify Requestor
Repeat Check Periodically
F
Requestor Provides Adequate Information
N
Close after Waiting Period

Figure 4: IANA Change Request Sub-process: Tech Check (Part of validating the request is well-formed, complete & meets objective assessment criteria)

The Tech Check process raised several questions, particularly through the survey of IANA customers:

1. What is the IANA purpose for performing Technical Checks and is that purpose met using the present scheme of performing Tech Checks during processing of NS and DS change requests only?

2. Competently operated TLDs often fail Tech Check due to timing issues, e.g., nameserver serial number updates that are routinely performed for security purposes.

3. Given the rise of Registry Service Providers in the marketplace, serving multiple TLDs, do Tech Checks need to be performed for every NS and DS change request (especially when issue #2 above often requires personal intervention by the RSP)? Is there a more efficient way to conduct Tech Checks that fulfills their objective?

Discussions with the IANA team and its customers exposed the complexity of these issues, which are addressed in the Technical Check Issues Discussion presented below. Briefly, IANA has already been involved with their customer community, developing a more efficient and meaningful Tech Check process.

In addition, our team had these questions relating to documentation:

1. Are there criteria for adequacy of the “requestor explanation” if Tech Check is failed?

   There are not written criteria but there are certain explanations, such as serial number updates, that are routinely accepted. While the experience and knowledge of the IANA staff ensures, to our satisfaction, that an inadequate explanation will not be accepted, we think that documentation should be upgraded to indicate:

   - which explanations are acceptable and the criteria against which they should be measured, and

   - a staffing escalation path indicating which staff members are authorized (after appropriate training and experience) to authorize root zone changes based upon explanations of failed Tech Check.

2. Are nameserver technical requirements periodically reviewed?

   The IANA team described changes implemented in the Tech Check process as RZM change requests and the DNS have evolved, demonstrating that the Tech Check process and requirements are routinely and regularly reviewed and updated. They are published here: https://www.iana.org/help/nameserver-requirements.

Ensuring Proper Authorizations Are Given by Designated Contacts

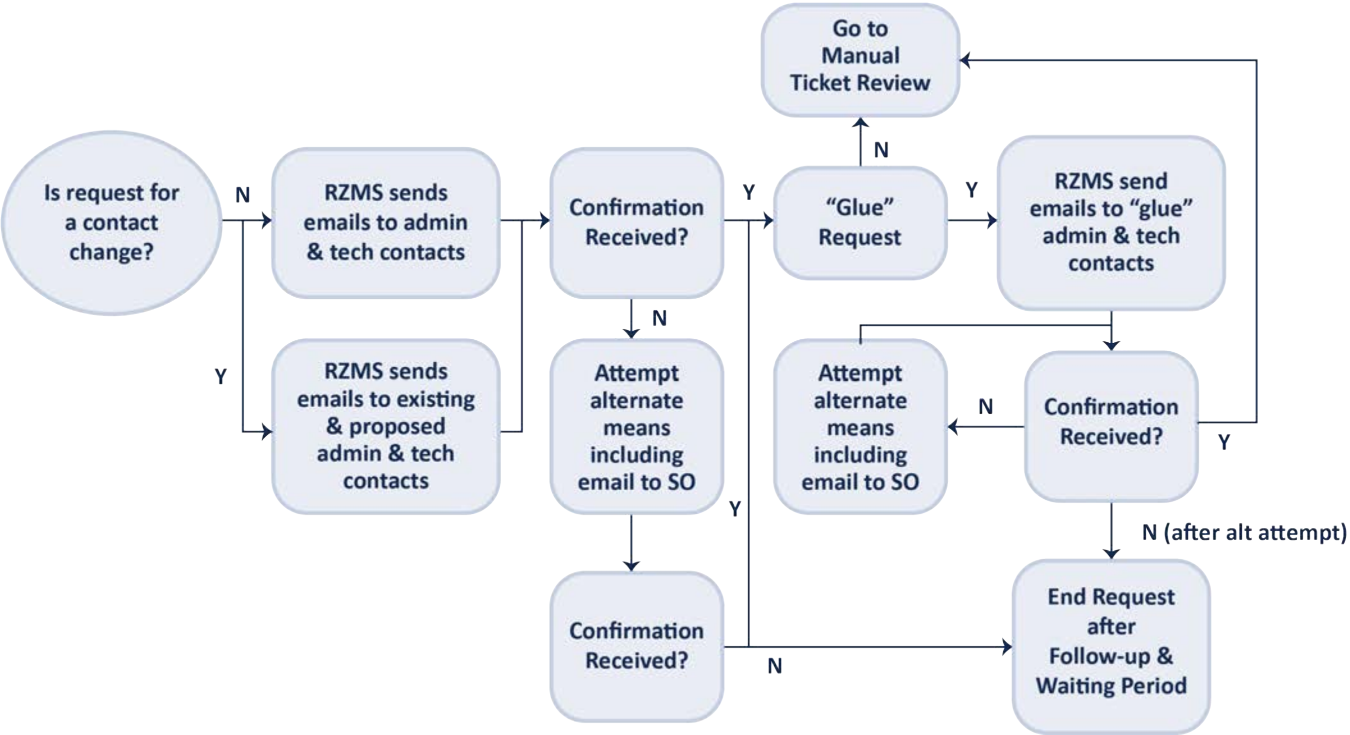

Go to Manual Ticket Review
Is request for a contact change?
N
RZMS sends emails to admin & tech contacts
Confirmation Received?
Y
"Glue" Request
N
Y
RZMS send emails to "glue" admin & tech contacts
Y
RZMS sends emails to existing & proposed admin & tech contacts
N
Attempt alternate means including email to SO
Attempt alternate means including email to SO
N
Confirmation Received?
Y
Y
N (after alt attempt)
Confirmation Received?
N
End Request after Follow-up & Waiting Period

Figure 5: IANA Change Request Sub-process: Ensuring proper authorizations are given by designated contacts

This sub-process confirms the identity of the requestor and ensures that cognizant TLD personnel authorized the requested change(s).

This sub-process addresses several different scenarios:

- If the request is for a change of Admin or Tech Contacts, then the old and new contacts must verify the change.
- If the change request is for a nameserver change and involves a provider that serves a number of TLDs, then contacts must be confirmed for all the TLDs using that same nameserver (also known as a "glue" request).
- Where Admin and Tech Contacts are not reachable, IANA uses either private emails, contacts through personal knowledge of the operation, or the publicly available contact of the Registry Operator / TLD Manager.

These scenarios gave rise to a set of questions from IANA customers and our team:

1. Are there any exceptions to confirming either both contacts *or* confirming through an TLD Manager?

   There are rare exceptions made with unusual circumstances that are handled on a case-by-case basis. While we prefer completely documented processes, in these difficult-to-anticipate cases, a final decision should be left to an authorised IANA team member. In such a case, the process documentation should indicate the team members that are authorised to approve these "out of band" contact confirmations.

2. What are criteria for approval based on contact with a TLD Manager?

   These are generally based upon the personal knowledge, industry experience, and acumen of the IANA staff. It is difficult to document the criteria for making these calls so the process documentation should include a list of authorized personal for these out-of-band authorizations, either by name or title.

3. Requiring all "glue" contacts to agree extends the time of or bars the change. Is there a more efficient method?

   Yes. IANA staff have already been collaborating with the community to enact a change in the standard for authorising a glue change. After years of processing glue changes, it has been recognised that these changes result in improved (i.e., more stable, secure) operations and there is little or no downside risk to approving them, even in the case of one or more parties not explicitly approving the change. IANA is planning to recommend a change to the processing of glue requests from "opt-in" to "opt-out" so that, after the requestor and one other TLD has explicitly approved the change, any TLD that does not object will be presumed to have approved the change. IANA is planning appropriate community discussion and safeguards in implementing the change.

One other finding of note came out of the customer surveys and interviews: that many Admin and Tech Contact points are stale or are people focused on other tasks. The reasons and recommended cures for this are described in the Customer Track portion of this paper and the relevant Issue Discussion section.

The overall recommendation for this section is that process documentation should be upgraded to include either criteria for approving "out-of-band" contacts or identifying the IANA staff (by name or position) of those authorized to do so.

Manually Reviewing the Requested Changes to Determine if Additional Information Is Required

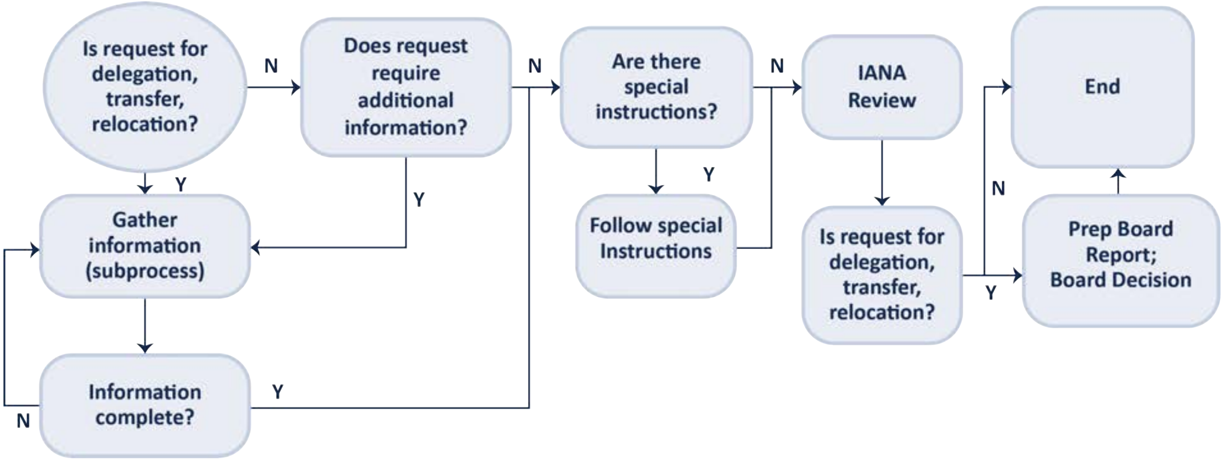

Is request for delegation, transfer, relocation?
N
Y
Does request require additional information?
N
Y
Are there special instructions?
N
Y
IANA Review
End
Gather information (subprocess)
Follow special Instructions
Is request for delegation, transfer, relocation?
N
Y
Prep Board Report; Board Decision
Information complete?
Y
N

Figure 6: IANA Change Request Sub-process: Manually reviewing the requested changes to determine if additional information is required and gathering additional information where required

While the RZM system automates much of the Root Zone Change Request process, the Manual Review provides the oversight necessary to ensure all documentation is complete and peculiar aspects of any requests are addressed. Changes of TLD control often require manual interventions, such as demonstrating government backing of a ccTLD re-delegation in certain instances. This part of the process provides proper IANA staff focus on the most impactful of change requests, changes of control.

The ICANN Board role in ccTLD changes of control was reduced in 2012 when the last US Government IANA contract was issued. It limited the ICANN Board to its current role to ensure that proper procedures were followed.[5] (Formerly, the Board considered IANA-recommended re-delegation requests more broadly and on the merits of the request.) The Manual Review process and Additional Information Gathering processes enable IANN staff to assemble an adequate dossier of documents for Board review.

The section of the Change Management Process also provides for any special regulatory requirements (for those familiar with the process, this includes potential U.S. OFAC reviews), and any other security checks under the task of "Follow Special Instructions."

During our review of this part of the process we sought to find unneeded steps and whether the separate process steps for handling requests of ccTLDs and gTLDs could be combined in some way. In the end there were no efficiencies to be realised in this area. One reason: the final "sign-off" of ccTLD Changes of Control is the ICANN Board, and for gTLDs, that role is taken by the Global Domains Division of the ICANN Organisation. Therefore, it is necessary to provide separate processing for each.

Completing the request

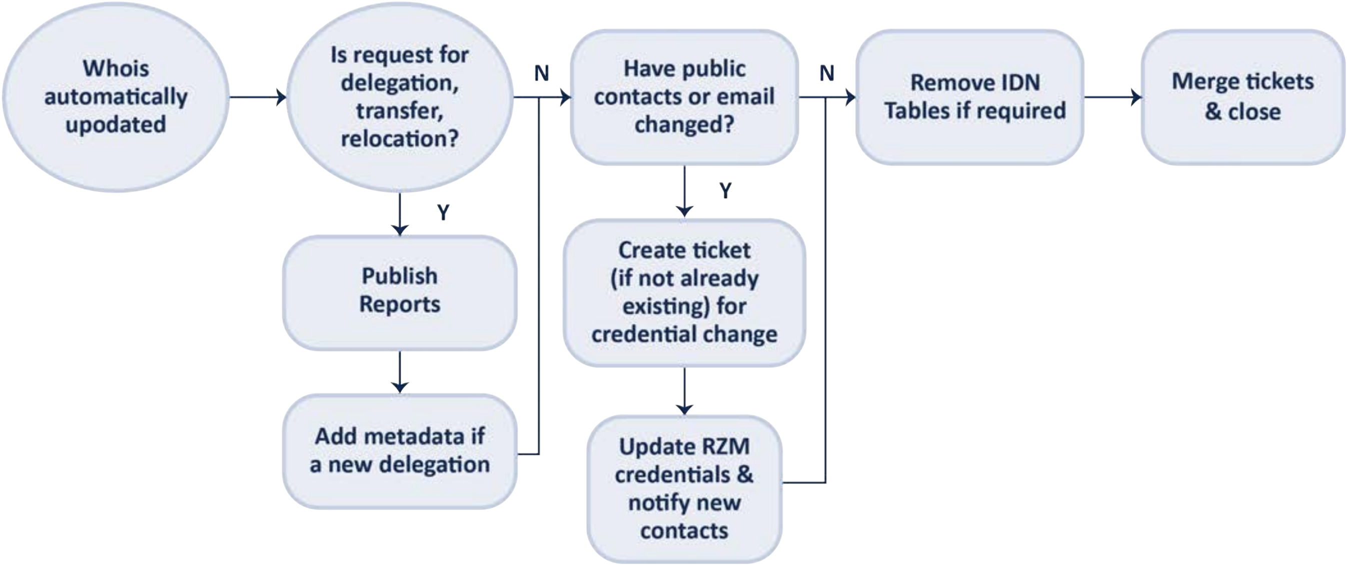

Whois automatically upodated
Is request for delegation, transfer, relocation?
N
Y
Publish Reports
Add metadata if a new delegation
Have public contacts or email changed?
N
Y
Create ticket (if not already existing) for credential change
Update RZM credentials & notify new contacts
Remove IDN Tables if required
Merge tickets & close

Figure 7: IANA Change Request Sub-process: Completing the request, ensuring that new / changed data, reports, and credentials are published into Root Zone file and other appropriate databases

This portion of the process ensures that new / changed data, reports, and credentials are published into the appropriate databases. The documentation provided by IANA clearly describes each step and each of those steps is necessary to complete the work.

[5] See https://www.ntia.doc.gov/files/ntia/publications/june_26_redacted.pdf, item 3.

The questions arising from this portion of the review:

1. Is there a final notice to the TLD manager?

   The process calls for a notice to be sent to new contacts (in the event of a contact change) but there is no notice to the TLD points of contact called out for other types of changes. In fact, IANA provides follow-up notices to the requestor and then makes a notification that the change request ticket has been closed. This is indicated in the overall Root Zone Management Change Request Process, even though it is not included in a sub-process.

2. Where are templates for reports and metadata stored?

   The IANA Process documentation contains links to internal information and supplementary documentation. The information is contained at that location.

Single Points of Failure: Discussion

Single points of failure exist in instances where a resource that supports the RZM change process fails and the absence of that resource irrevocably leads to a failure of the process. We examined the two sets of resources that support the RZM change process:

- staffing, and
- process documentation.

(We also examined IANA Systems for single points of failure. The methodology and results of that investigation are in the Systems & Architecture section of this paper.)

1. Staffing:

   a. For each process step (and for each type of root zone change request), we identified the staff members that would be assigned to that step and the staff members who could perform the required tasks in that step if the original assignee was not available.

   b. We verified current ICANN org charts, understanding each staff member's time-in-grade, geographic location, and experience level so that we could understand the available pool for each assignment.

   c. Through discussion with IANA leaders, we learned IANA's professional development track to understand the evolution of staff capability to handle assignments of increasing complexity over time.

   d. We used IANA public reporting, discussions with staff and interviews with customers to understand the IANA workload.

   With that information, we were able to make determinations about the ability of the IANA staff to withstand certain stressors and still perform the IANA Change Management function in a timely, competent manner.

   The analysis, determinations and recommendations can be found in the Issue Discussion entitled IANA Staffing, which can be found below. Briefly, we find the staffing, in numbers and training to be well-matched with the need (i.e., adequate with appropriately sized redundancy). We also recommend that the geographical diversity of the staff be increased (with certain limitations) to improve resiliency.

2. Process Documentation:

   a. We requested and received process documentation governing the Root Zone change request process. That documentation is published on the inward-facing IANA website, and a portion, in unannotated form, in the appendix to this paper.

   b. Using only that documentation (and some knowledge about the Root Zone Change Management process), we attempted to construct (in a table-top manner) the Change Management process.

   c. Where there were "process blanks" in the documentation, the IANA staff provided the necessary information during our meetings with them. We were seeking not just to "fill in the blank," but to understand how the IANA staff would find the answer, i.e., through colleague consultation, training, other documentation, or learned experience.

Starting with an admittedly idealistic model that IANA documentation should be sufficiently complete so that a member of our ICJ team (i.e., a person with some knowledge of IANA processes) could use the documentation to successfully execute a RZM change request, we identified improvements that can be made to move closer to that standard. The recommended changes are in the area of augmenting decision criteria to determine whether submitted requests fulfill all the informational requirements and what additional information would be required to make the requests complete.

The analysis, determinations and recommendations can be found in the Issue Discussion entitled IANA Documentation.

SYSTEMS & ARCHITECTURE TRACK

IANA Principle: to ensure that IANA processes are secure, stable, and resilient to accidental or malicious change.

Objective of Track

The objective of this track is to investigate whether there is a need to increase (and if so, how) the robustness of the operational arrangements for making changes to the root zone content, identifying any single points of failure that may exist and, should they exist, offering recommendations on how to mitigate or eliminate them.

While the study scope is described in detail in the Introduction, it is important to note that this study does not address any systems or processes surrounding DNSSEC signing of the root or any processes or procedures involving DNSSEC aside from the routine process of TLD managers submitting DNSSEC-related records to IANA for inclusion in the root.

Methodology

This report section relied on the IANA customer survey and interviews, interviews with IANA staff using prepared questions targeting the study objectives listed below, review of IANA process and systems documentation, review of third-party audit results, and answers to a set of questions asked of Verisign. Verisign's initial response to these questions indicated reticence to furnish security-sensitive information that might become part of a public report. Since the purpose of this report is to publish findings to the broad ICANN Community, ICJ tailored the questions asked of Verisign. Verisign furnished a response that contributed to the findings in this report; the revised questions asked of Verisign and their responses are provided in complete form in the Appendix.

Our methodology followed that of a typical systems and architecture analysis:

1. Clearly state the specific hazards and security/risk objectives we wish to measure. These are enumerated in the RFP.

2. Create a Threat Model to enumerate the vectors that could lead to those specific hazards being realized or the security/risk objectives not being met

3. Analyze the controls in place to determine how adequately they reduce the probability that the vulnerabilities identified in the Threat Model could be exploited

4. Assess if the resulting level of risk is acceptable. If not, recommend additional controls. If risk is over-managed, recommend controls that may be removed.

Results and Findings

In general, ICJ finds that the operational systems are "right-sized" given the task, load, and risks at hand. We do not find that risk is materially under- or over-managed (requiring a significant increase or decrease in controls). In the spirit of incremental improvements, we do make several recommendations over the course of the following pages.

Discussion of the IANA Customers

There are several different types of TLD operators that may interact with IANA with differing use cases. TLD operators themselves vary widely from small Country Code (ccTLD) Operators maintaining only a single ccTLD to large TLD operators that maintain dozens or hundreds of TLDs for themselves and potentially on an outsourced basis. This wide range of customers necessitates that IANA service large, high volume, sophisticated TLD operators that may require several changes per zone per year to very small ccTLD operators that may only request a change every couple of years.

The implications of the interaction models are significant. For example, a large, sophisticated TLD operator interacting with IANA several times per year might have staff trained and familiar with IANA processes, might have credentials to the IANA RZMS, understand the performance of the process, and have expectations and experience to guide them. Said differently, there is a level of persistent institutional knowledge about the IANA processes within the sophisticated TLD operator that spans time and multiple requests.

At the other end of the spectrum, a small TLD Manager that only submits a request once every several years may have near zero persistent institutional knowledge about the IANA processes. Long time periods (and staff turnover) may create a situation where every time the TLD operator makes an IANA request, there is limited or zero institutional knowledge/familiarity, creating an “every time is like the first time” scenario.

This spectrum of customer interactions presents challenges to IANA and impacts everything from system design, request intake, and performance of identification, authentication, and authorization functions. The concept of serving a range of very different clients appears several times in this study and is quantified in the Customer Communication Track.

Description of the Processes

IANA Staff, supported by several IT systems, perform the functions defined in the process. Additionally, one third party, currently Verisign, supports the Process in a contracted role as the Root Zone Maintainer (“RZM”), a role it as performed for decades.

These processes are described in detail earlier in this study. For the purposes of this section, it is important to know that all Root Zone Change Requests (the “Request”) are initiated as an inbound request from a Requestor. In theory anyone may request a change and the initial request may arrive via email, phone/fax call, or through the ICANN-developed Root Zone Management System (“RZMS”) Ticket. Robust authentication and authorization of the Request are performed in later steps of the process. IT workflow systems guide the request through a series of steps with dependencies on human processing, culminating in a technical exchange with Verisign wherein the request is set for implementation.

Threat Model

The RFP requires the study to address the following questions:

a) The potential for accidental or malicious changes or omissions by the IFO or Root Zone Maintainer.

b) The potential for out-of-policy changes by the IFO. The term “policy” is used in its most general sense, representing formal Policy adopted by ICANN as well as established standards, practices, and processes.

c) The potential for accidental or malicious errors in the communications path from the IFO to the Root Zone Maintainer.

d) The potential for accidental outages or malicious actions related to the telecommunications infrastructure serving the IFO and the Root Zone Maintainer. Such outages or actions could be related to the infrastructure shared with ICANN.

A Threat Modeling approach is a useful tool to explore these very specific threats or loss scenarios and complements the existing Systems/Controls-based audits that are already performed (e.g., SOC2). ICJ uses concepts and terms from NIST Special Publication 800-154.[6]

The following sections discuss the generalized Attack Vectors that could lead to one or more of the specific loss scenarios described above. The term “Out of Policy” is a general term used by IANA to indicate a change that was not intended, or not consistent with or supported by IANA Policy. While exploring these specific loss scenario hypotheticals, we individually consider the source where the unintended change originated then consider the mechanisms in which the change could have been introduced.

In the case of hypothetical unintended changes introduced at IANA or at the Root Zone Maintainer (Verisign), the threat models are very similar. This is not unexpected as both IANA and Verisign depend largely on expert, trustworthy humans supported by a relatively small number of software tools and systems.

It is critical to note that these threat models enumerate the potential sources of unintended changes to the root zone. Both IANA and Verisign have controls in place to reduce the likelihood that unintended changes are introduced and to detect the introduction of unintended changes and limit their damage.

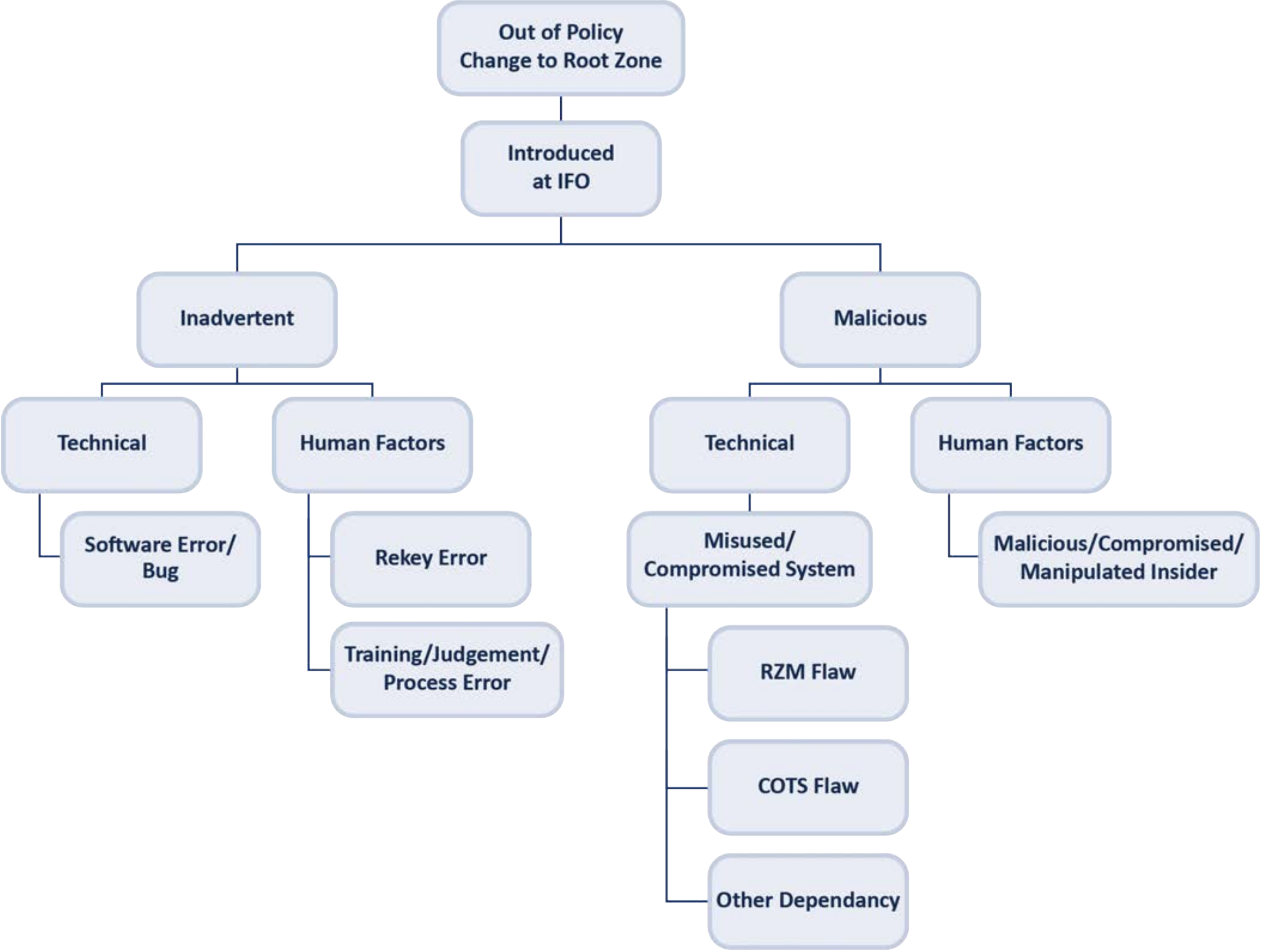


Figure 8: Loss Scenarios (IANA)

[6] https://csrc.nist.gov/CSRC/media/Publications/sp/800-154/draft/documents/sp800_154_draft.pdf

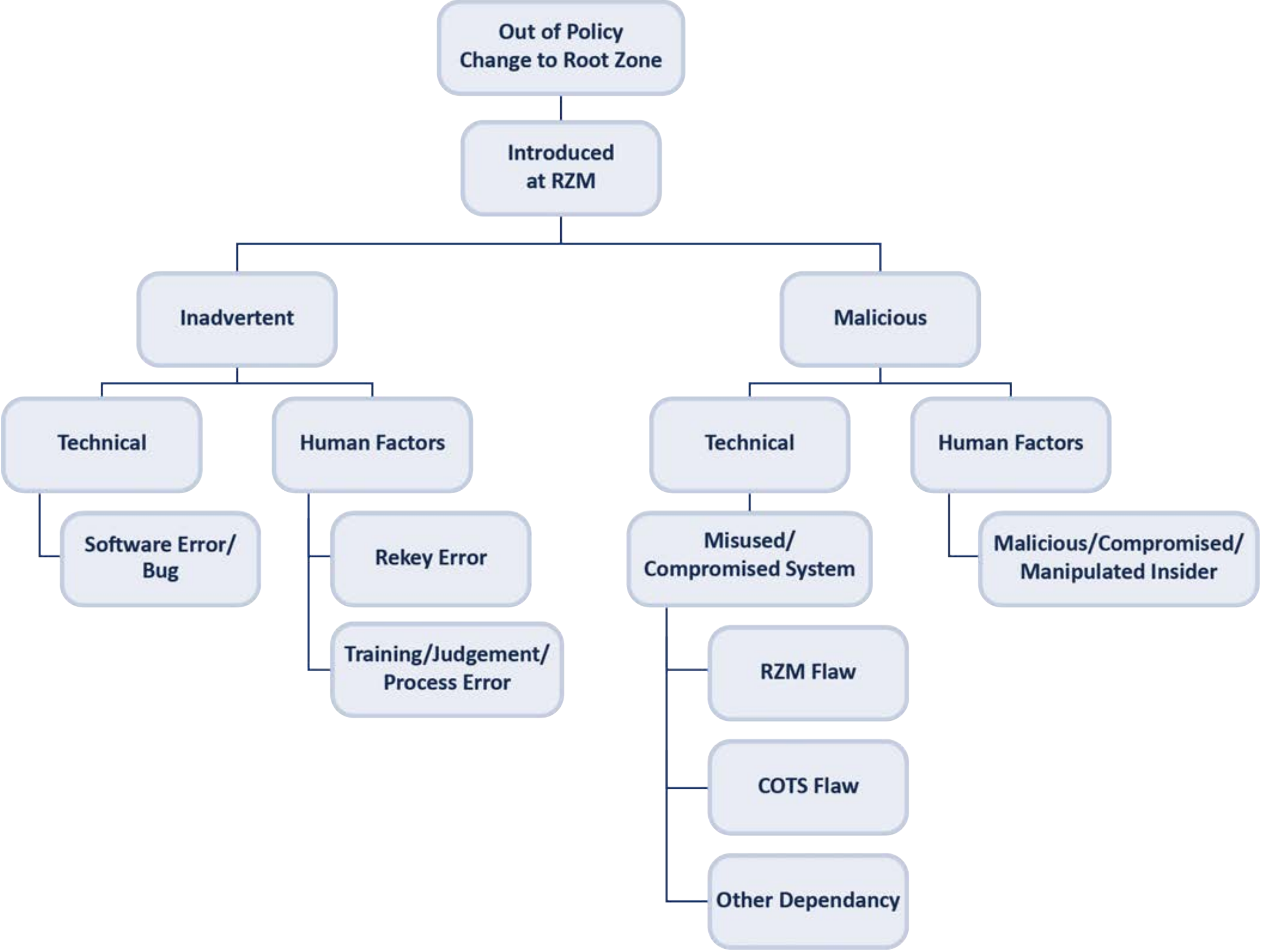


Figure 9: Loss Scenarios (Root Zone Maintainer)

We discuss the components of the threat models in the following sections.

General Controls and Practices

Both IANA and Verisign leverage general controls and practices that greatly reduce the probability that an error – whether inadvertent or malicious – could be published in the root zone.

Systems Controls

Both IANA and Verisign deploy a suite of controls based on industry standard IT controls frameworks including: NIST Cybersecurity Framework (CSF), The Center for Internet Security (CIS), and NIST 800-53, among others. Additionally, both IANA and Verisign have these controls validated by third parties using the System and Organization Controls (SOC) 2 framework developed by the American Institute of Certified Public Accountants (AICPA). SOC2 Type II audits provide attestation from independent, third-party auditors concerning the existence and operating effectiveness of controls. Additionally, as a publicly traded company, Verisign is subject to numerous other control audits, disclosure requirements, and compliance regimes.

ICJ has reviewed the SOC2 reports covering the IANA system – which specifically includes the RZM System in-scope – and found them to be as expected and consistent with industry norms. SOC2 audits for Verisign were not requested nor received.

The types of controls reviewed in SOC2 type audits are best characterized as general-purpose good IT hygiene controls. They include topics such as: authentication/password requirements, account provisioning and deprovisioning, and secure deletion of data. Additionally, SOC2 also covers certain Governance, Risk, and Compliance (GRC) topics such as executive and Board oversight of IT risk. These controls form the essential baseline for operation of secure and robust IT systems.

The existence of audited and validated IT controls in general reduces the probability of a wide range of inadvertent and intentional actions. Our intent in this study is not to rehash these baseline audits but rather to expand the analysis to include discussion of specific threats, risks, and mitigations unique to the root zone change process.

> RECOMMENDATION: IANA should consider rotating SOC2 auditors in this year's rotation.
>
> RATIONALE: ICJ notes that the same external firm has completed the previous three (3) plus the current SOC2 Type II audits for IANA. While not strictly required – and recognizing there are some benefits to working with the same firm for multiple assessments – it is good practice to rotate auditors and obtain a "fresh set of eyes" on systems after several years. We note that IANA has rotated vendors though an ICANN public RFP process every 3-5 years and so are indicating that this practice should be maintained. Meetings with IANA and ICANN procurement staff indicate that this will be the case.

Low volume, reviews, checks, and "Two Person Rules"

As a general statement, the root zone change process is a relatively low volume process. On average, a TLD will submit one to two requests per year. Recent industry consolidations have driven up the number of requests given the reorganization of technical infrastructures. With these effects, IANA has fulfilled 4600+ change requests over the past 12-month period. Even this volume allows for a very high level of verification and review by multiple parties. This verification and review serve as broad protection against a range of inadvertent and malicious activities.

Recalling that the Root Zone Maintainer was furnished with an edited set of questions, Verisign, in their response describes *Manual review and approval to publish by at least two Verisign staff members.* Elsewhere in Verisign's response, they describe the separation of privilege principal they employ: *…separated privilege between two types of access: access that provides the ability to introduce change, and access that provides the ability to approve change. The system enforces that these two types of access are mutually exclusive; to gain one is to lose the other.* Additionally, the IANA process requires at least two individuals to approve the request prior to passing to Verisign. Taking those in sum, at least four distinct individuals across two organizations will review each change request. This is an extremely powerful control against a full range of inadvertent and intentional errors.

For clarity, however, *Verisign does not exercise any independent editorial actions of the root zone and does not check change requests for policy correctness. Verisign does evaluate each RZCR for technical accuracy and impact. On rare occasions an RZCR may enter a temporary hold state while Verisign seeks additional guidance and confirmation from IANA* (text from Verisign Response). While at least four individuals will evaluate each individual request for technical correctness (as well as a general "sanity check"), only the individuals from IANA will also evaluate for policy compliance. We call this out only for clarity, not as a concern, as it is consistent with the designed division of duties among and between the IANA and the Root Zone Maintainer.

Low volume expert-driven processes are often vulnerable to social engineering and other human factors attacks and must continuously be on-guard against complacency. Process formality, workflow systems such as RZMS, and well documented processes for emergency interactions mitigate these dangers. Both Verisign and IANA describe formally documented emergency procedures and drive any 'abnormal' workflows to formal ticketing and workflow systems. These serve as controls against human factors attacks and complacency.

Pre-publication of records in TLD zone

IANA requires that all records technically capable of being pre-published in the TLD zone prior to publication in the root are so published prior to passing the request to the Root Zone Maintainer. This is an extremely powerful, general-purpose control that defends against a wide range of inadvertent and malicious activities.

Most notably, this control requires the requestor to have *a-priori* control over the TLD zone the requested change impacts. This is a powerful authorization mechanism and, in all but the most obscure hypotheticals, ensures that the requestor is authorized to request the change. Additionally, it is a powerful control against inadvertent errors as it allows programmatic comparison of the requested record change to the 'reference' record already published in the TLD zone. This is an unambiguous check performed by both ICANN and Verisign during their technical checks.

Maintaining this control drives some of IANA's behaviors, we believe rightly so. For example, a small minority of IANA Customers during our interactions expressed displeasure that IANA does not allow the TLD Mangers to use the "double-ds" method of rolling DNSSEC Keys. More specifically, IANA requires the TLD Manger to list the entire set of DNSKEYs in their zone apex prior to making root zone changes. This ensures that the TLD Manger must be in control of the zone they are impacting, as well eliminating the risk that a DS record is entered incorrectly (which is not verifiable by IANA *a-priori*). This example is not hypothetical – it has occurred. In two previous instances IANA waived the pre-publication requirement on an individual case basis, only for the TLD Manger to roll their key and then have the TLD become unresolvable because the DS record supplied was wrong. This required an emergency root zone change to resolve. This issue is discussed in greater detail later in this study.

Monitoring and global visibility

While not a traditional control, it bears mentioning that the global Internet DNS root is among the most closely watched and monitored systems on earth. Numerous parties analyze and report on every change to the root; there are even multiple Twitter bots that report on root zone changes. Importantly, each TLD Manager has the ability – arguably the obligation – to proactively monitor the root for changes impacting their zone. Because of this, any unintended change – whether intentional or malicious – is both able and likely to be detected quickly by numerous parties, including the parties able to initiate corrective actions. The larger and more critical the TLD, the more likely rapid detection of an error becomes.

In the case of a DNS error, the damage is proportional to the time the error exists before it is corrected. In the event of a delegation or a DNSSEC publication error that causes an entire TLD to go offline, the extreme impact makes detection nearly immediate, and remediation would be carried out on an expedited basis by all parties. In the case of the root zone, nearly all conceivable errors would be of this gross delegation variety causing a TLD to cease functioning. While high impact, it will likely get corrected quickly, somewhat limiting the damage.

Not to say that even brief outages are at all acceptable. An outage of even a few minutes on a critical TLD could have immeasurable global economic impact. Rather, we state that root zone DNS changes – be they intentional or unintentional – cannot by their very nature be surreptitious. They can and very likely will be detected quickly, bounding the damage.

Please be reminded that this study does not cover the generation and maintenance of DNSSEC keys or any signing operations. Errors involving the generation of cryptographic material and signing operations can be far more insidious.

Software Error/Bug

In any software system, there is always a risk that errors – either in design or in implementation – may cause unexpected results. In the case of the root zone change process, a combination of commercial off the shelf (COTS) and custom software is deployed at both the IANA and the Root Zone Maintainer; flaws in this software could lead to the introduction of an out of policy change.

In addition to the general controls above, several specific additional mitigations and controls exist to reduce the likelihood of this occurrence and are discussed below.

Requirements and Design

Reliable and secure software starts with good design and security requirements. While ICANN has a formal methodology to guide development of applications and systems and several processes exist within ICANN's E&IT, a formal and documented Software Development Lifecycle (SDLC), inclusive of upfront security and resiliency requirements, does not exist. ICANN architects and developers are certainly well aware of the importance of security and numerous security-related steps are undertaken (including regular vulnerability scanning, SOC2 Type II audits, and external penetration testing of the RZMS web application), but documentation of upfront assumptions and requirements are informal. Additionally, no specific mention or culture of secure coding practices, "Secure DevOps," or other proactive practices could be identified.

> RECOMMENDATION: IANA, in conjunction with ICANN E&IT, more formally document assumptions and requirements for the custom developed software (specifically RZMS).
>
> RATIONALE: The process of developing security requirements and assumptions helps developers and operators alike align on the expectations, costs, and ancillary requirements (such as monitoring and response capabilities) required to fully support custom software. One minor issue identified during IANA customer interactions – the use of persistent URLs with embedded security tokens – would likely have been identified during an upfront security design review as secure development best practices usually contain discussion about the dangers of such design patterns.

The Verisign response describes a strong GRC function and a culture that values and practices the formal aspects of information security and risk management. While not specifically requested by ICJ nor described in their response, we believe it reasonable to assume based on their other commentary that Verisign employs a robust software design and security requirements process for the custom software they develop to support the RZM process.

As a second line control against the full range of software errors, both the IFO and the RZM describe a practice and documented functions including human reviews, "two-person" checks, and two tiers of automated checks (performed by both the IANA and the Root Zone Maintainer). These checks are described in the Verisign response as well as in IANA documentation. These second line controls increase the probability that an unexpected change introduced by a software error would be detected and would not complete the process and be published in the root zone.

IANA also employs an extremely specific and useful control and practice that reduces the probability of a full range of inadvertent and malicious activities, including software bugs or errors. A root zone change must first be published in the TLD's zone before IANA will release the change to the Root Zone Maintainer for publication. This practice is described in the General Controls section.

Software Testing

ICANN performs internal testing, routine vulnerability scanning, and engages a third party to perform a penetration test (scoped to strictly test the software) on the RZMS system annually. ICJ has reviewed these reports and finds them in line with expectations and industry norms. Similarly, Verisign discusses software testing in their response.

Rekeying Errors

Processes dependent on humans have the potential to generate keying/typographic errors. IANA and Verisign attempt to drive-out rekeying errors using workflow systems and exchanging information programmatically via the EPP protocol. Based on documentation and discussions, it seems extremely unlikely in any but the most improbable artificially contrived scenarios that a human rekeying error could occur in the process as currently specified.

Training/Judgment/Process Errors

Human judgment errors are an area of focus given this specific process. Human judgment may be expanded to include inconsistencies and timeliness factors that, while not strictly security issues, may be customer service or perception issues.

The role of human judgment is essential as the IANA occasionally deals with unusual, unpredictable, and unforeseeable situations where extensive *a-priori* documentation is simply not reasonable. For example, natural disasters, global geopolitics, and technical emergencies drive many of IANA's unusual – and potentially more urgent – requests. In these situations, relying on the judgment and instincts of expert staff is essential.

IANA recognizes that their process is dependent on human judgment (and the consistent application thereof) and mitigates these risks through documentation and cross training. We find that the processes themselves are well documented at a high level, tooling is used to guide consistency, and that multiple staff members would likely independently reach the same conclusions in most routine scenarios. Additionally, multiple staff are trained to perform most functions, although there is a question about the extent this training is solidified with practice to mitigate skills atrophy.

We find that documentation of historical rationale, practice, and "case law" is lacking and exists largely in the minds of a small number of key staff. As such, while the risk of a judgment error or inconsistency is relatively low for routine requests, it is somewhat higher for complex or unusual requests. Non-availability of key staff (for any reason) would exacerbate such a scenario and may in the extreme introduce delays or inconsistencies with historical practices. Historical decisions and rationale for unusual scenarios could in many cases be reconstructed by reviewing tickets and correspondence, but this process would be lengthy and may delay processing.

> RECOMMENDATION: Establish a lightweight, searchable repository of "case law" to memorialize historical decisions and their rationale.
>
> RATIONALE: A simple wiki-type format organized by issue or scenario to capture historical practices and rationale would assist in rapidly determining a course of action in unusual circumstances. Capturing this knowledge – currently in the minds of a few key staff – would facilitate training, exercises, and improve IANA's resilience to staff turnover. Implementation and maintenance of such a system would not be materially costly.

By the nature of their role, the RZM is less susceptible to errors of human judgment as their role is limited to technical validation and publication. Based on Verisign's response, they have invested in tooling, process, and implemented a highly proceduralised system to largely drive out reliance on human judgment and the potential for human error. In their response, Verisign states that: *...nearly all processes and functions are fully automated to avoid human error...*

Employee background checks, ethics training, and related functions are also controls against human judgment errors. IANA performs background checks on all new staff and temporary employees in accordance with relevant laws, regulations and proportional to the business/security requirements. IANA employees are also required to complete security awareness training, anti-bribery, and anti-harassment training on a recurring basis. An anonymous hotline is available to staff to report any work-related concerns regarding ethical, moral, or legal conduct.

Misused or Compromised Systems

These risks are based on an active adversary able to use a system in a way not intended or authorized. This may come about due to the compromise of an underlying system/host, a flaw in software (COTS or custom), or the compromise of some other dependency that allows an attacker to obtain a level of trust or access that is not authorized.

IANA systems are supported by ICANN's IT department which has industry standard administration/operational procedures that are largely described and validated in the SOC2 Type II reports reviewed by ICJ. Relevant policies include: ICANN Engineering & IT Information Security Policy, Acceptable Use Policy, Access Management Policy, Data Classification Policy, Password Policy, and Incident Response Plan. These policies and practices are the first line of defense against system compromise or misuse.

Monitoring and rapid detection of malicious activity is an essential component of any defensive program. Like fire impacting a physical facility, the sooner an information security event is detected and contained, the less damage will occur. While ICANN monitors for traditional IT operational status, monitoring specifically for security events appears uneven. Moreover, it does not appear as though ICANN routinely tests its detection and response capabilities through tabletops or offensive testing ("red" or "purple" team testing) which exercise a full range of defenses, including detection and response capabilities. Mean Time to Detect (MTD) and Mean Time to Respond (MTR) objectives are not documented.

ICANN provided evidence of periodic vulnerability scans and references "scanning" activities in several places in their documentation, but these activities do not appear to exercise detection and response capabilities. Moreover, the "penetration tests" on the RZM system – while performed by a highly reputable firm – appear to be scoped as strictly software tests, not tests that would invoke ICANN's detection and response capabilities.

ICANN also provided examples of their periodic business continuity exercises and their continuity of operations plan, here too these artifacts and exercises did not involve scenarios where a potential system compromise was in play necessitating ICANN invoke incident response detection, and response capabilities.

Controls, including detection and response processes, must be routinely validated. Absent this validation, unfortunately, many IT controls simply do not function as documented or expected and can lead to undesirable situations.

> RECOMMENDATION: ICANN test security controls, detection, and response capabilities through a targeted offensive exercise program. Good offensive exercises (conducted in both "red" and "purple" formats)[7] are scoped to test specific assumptions; ICJ recommends that ICANN consider testing the following:
>
> Validate the level of isolation between critical IANA functions and the broader ICANN company systems and employees.
>
> Validate the ability to timely detect and respond to a suspected compromise of a critical IANA system. Validate roles, responsibilities, and processes in the event of a suspected compromise.
>
> Validate the ability to recover and re-establish trust in a critical IANA system following a suspected compromise.
>
> Test the potential to circumvent two-person rules by IT administrators and through social engineering vectors.
>
> Validate interaction with cyber and business continuity insurance carriers, their subcontractors, and contractors on retainer for incident response.

[7] A "red team" engagement is an offensive engagement where the defenders ("blue") are not aware of the test. These engagements test controls, detection, and response capabilities. "Purple team" engagements are conducted with the attackers and defenders working in partnership to validate and improve defenses.

> RATIONALE: Untested security controls and policies create a false sense of security, and many security breaches are founded on the belief that certain controls function in ways that they do not. Moreover, time to detect and time to respond to a potential cyber incident must be understood, measured, and validated as a part of an organization's overall risk management strategy.

In their response, Verisign describes their use of industry standard control frameworks and routine testing of the systems involved in root zone management and publication. Importantly, Verisign describes a number of detection and response capabilities, their use of red team exercises, and a 24x7 Network Operations Center (NOC).

Malicious, Manipulated, or Compromised Insider

Insider threats – specifically the unauthorized use of authorized access- are among the most difficult risks to address in the modern IT centric work environment. IANA primarily addresses the potential of an insider threat with robust two-person rules making it impossible for a single person to push a request all the way through to Verisign for publication. While this is good practice, it is unclear to what extent IANA's two-person rules are protected from being overridden by IT department administrators or extremely well trusted individuals on the IANA staff. These scenarios would be good fodder for offensive exercises as suggested previously.

IANA also addresses insider threats with the HR policies discussed previously. IANA does not have a specific insider threat program beyond what is described here.

In their response, Verisign describes a number of controls that reduce the probability that an insider threat could affect a root zone change. Verisign states that their insider threat program is modeled after the Carnegie Mellon SEI insider threat program, which CMU co-developed with the FBI and is well respected in the industry.

Architecture and Design

The IANA root zone change process is largely a clerical process that responds to requests from TLD Managers, verifies the authenticity of the request and the *authorization* of the individual making the request, performs technical checks, and passes a successful request to Verisign for publication. The process waits on any necessary confirmations, clarifications, or issues until it is completed successfully, withdrawn by the requestor, denied, or times out.

The process is dependent on the RZM system, which is a custom developed software system written by the ICANN IT department, to support this process. RZM, together with the ticket tracking system RT, manage request workflows, interactions with the requestor and other involved parties, and at the culmination interaction with Verisign over EPP. Email and phone communications are supplemental at all phases of the process and used as required.

From an IT perspective, we find the systems to be well designed and built for robustness. Much care in the design of the systems is taken to ensure that system availability is high – even during significant disruptions. The systems are run out of two physical datacenters – one on each US coast – and failover and failback exercises are routinely performed. We have reviewed the results of several technical failover and business continuity exercises and found them to be as expected and appropriate.

The SOC2 Type II audits we reviewed are scoped to cover the RZM and upon review we found them to be as expected and appropriate.

FINDINGS, RECOMMENDATIONS, & RATIONALE (ISSUE DISCUSSIONS)

Introduction

The information developed during the execution of the three "tracks" described above led our team to the conclusion that, five years after separation from NTIA oversight, IANA is a well-operated, highly regarded service provider with a track record of continual improvement.

In certain cases, the information we learned invited additional analyses to determine if there existed possible single points of failure, redundancies, or cost-justified opportunities for improvement in the Root Zone Management change process. The ICJ team, communicating often with the IANA staff and its customers, identified seven areas for additional study. Each area was briefly described earlier in this report and those discussions are fleshed out below. For each issue we: provide background information, describe our findings, make specific recommendations, and provide rationale and cost-benefit analysis to support the recommendation.

Authentication (Multi-factor)

Issue

Should multifactor authentication be required for Registries to login to RZM?

Background and Findings

Several survey respondents mentioned that IANA does not use multifactor authentication to authenticate access to the RZM system. Perhaps driven by the prevalence of multifactor authentication in other personal and business environments, the suggestion was made that IANA should also use multifactor authentication. Current IT practice drives the perception that multifactor authentication is appropriate (and expected) for high security applications such as online banking and business applications; ICJ believes this perception also drives a viewpoint that a critically important function such as root zone management should also be protected by multifactor authentication.

Given its mission, authentication in the IANA RZM context is a complex issue, not lending itself easily to the deployment of multifactor authentication tools with which we are familiar. This is exacerbated by the IANA principle that anyone can submit a Root Zone Change Request and so IANA cannot provide authentication credentials to unanticipated users of the system.

We explore the issues, use cases, and net impacts to security and usability.

Credential issuance, reuse, and "trust reboot"

Most internet users are familiar with the online banking use case: a long-lived credential (username and password), together with a second authentication factor (e.g., token, facial recognition, SMS), authenticates access to a website or application that the user visits frequently. The relationship between the user and their bank typically spans many years. A similar use case exists for online business services such as Office 365, VPN access, and other systems that users employ professionally.

Contrast this use case with the TLD manager/IANA relationship. A TLD manager submits zero to only a few requests to IANA annually, and often TLD manager staff have changed between IANA submissions. This requires IANA to "reboot" the trust relationship in some way, e.g., confirming the individual is authorized to make the request on behalf of the TLD, creating or resetting the user's (possibly forgotten) username or password, or processing a user's change of email address. The RZM/IANA use case varies from the traditional multifactor authentication use cases in that IANA additional authentication and authorization checks – beyond username and password- are already a part of the typical process.

The IANA processes for verifying or re-establishing trust with a TLD manager employee depend on the specific scenario at hand and range from relatively straightforward password resets to leveraging Governmental Advisory Committee (GAC) contacts to verify TLD personnel. Establishing trust with a TLD employee often involves multiple forms of communication (voice, email, web application, written letters) spanning days or weeks, thereby making circumvention more difficult. The increasing practice of outsourcing operational functions to Registry Service Providers necessitates IANA perform additional verification of authorization prior to making root zone changes including interacting with TLD manager business contacts of record.

Compensating Controls

When viewed end-to-end, the root zone change process incorporates several layers of controls that substantially reduce an attacker's ability to leverage a weak initial authentication. Unlike a bank transaction that may occur instantly, the root zone change process spans days or weeks prior to any change being implemented in the root. This reduces the probability that an attacker – even if successful exploiting a weak initial authentication – could complete the process and cause a change to the root. Expedited emergency processes as implemented by both IANA and Verisign are specifically engineered to maintain the same level of confidence in authentication and authorization functions as the non-emergency processes.

The most operationally impactful changes to the root – changes to published DNS Resource Records – require pre-publication of the requested changes in the TLD manager's servers prior to changes being implemented in the root. This control requires the TLD manager requesting the change to demonstrate control of their TLD zone prior to the requested change being published in the root. This is a powerful control against errors and malicious activity.

Expert human interaction and review throughout a process spanning days or weeks and separation of duties among multiple individuals and multiple institutions, are the ultimate backstops against a full range of threats to the system whether intentional or unintentional.

Additionally, the internet's root zone is one of the most heavily monitored systems on earth. Numerous parties monitor every change to the root zone, and nearly all TLD operators explicitly monitor changes to the root zone that impact their operations. Any erroneous change – whether intentional or unintentional – would be detected and remediated quickly. Almost certainly within a few hours. While the operational impact may still be enormous, there is a small- and finite-time window that an erroneous root zone publication would survive.

Data Leakage

Aside from causing a change to the root zone, it is important to consider what other data/processes a malicious party could access with a false authentication. ICJ became aware of scenarios where a stolen or compromised credential and/or HTTPS links with embedded authentication tokens may allow an attacker to view completed and/or in-process IANA/RZM tickets, Registry contacts, and other supplemental information. While accessing or manipulating such data does not directly lead to an unauthorized change to the root zone, leaking such data could facilitate social engineering or other attacks on Registry systems or personnel. ICJ has provided IANA with additional technical information about these scenarios and strongly recommends that no information be available from RZM absent an appropriate authentication and authorization.

Cost-Benefit of Multifactor Authentication

Deployment of multifactor authentication is complex and expensive. One must consider the direct costs of the tokens/hardware/software/service required to implement the system as well as the ongoing impacts to operational and support costs. Banks in the United States estimate that 30% of their help desk/support calls are credential-related and the complexities with multifactor authentication exacerbate the support issues and costs. One way institutions have sought to address costs associated with credential support is the use of self-service username discovery and password reset techniques. These techniques – with which we are all familiar – allow the user to reset a credential without contacting a help desk. However, in the unique IANA/RZM use case, deploying self-service techniques would likely reduce the overall level of security as currently trust reboot issues are dealt with manually and rigorously as discussed previously. Given the global scale of IANA's users and the frequent reliance on a full range of manual trust reboot procedures, traditional self-service techniques are not appropriate for the IANA/RZM use case.

Selection of the second authentication factor is complex in the unique IANA/RZM use case. IANA cannot assume that every global user of RZM has access to a mobile device onto which they can install an authenticator application. Codes delivered by SMS text messages have significant security and usability issues that are exacerbated when considering deployment on a global scale. Depending on implementation specifics, using codes delivered by email as the second authentication factor could add to the overall level of security.

Using an identity service provider such as Okta is an option, but such a path would dramatically increase IANA's cost, increase the risk surface area with new dependencies on complex third-party systems, and create little if any net increase in security in the overall root zone change process.

Noting the fact that the TLD manager controls their own zone, one possibility for a second factor is publication of a public key in the TLD's zone and using that key pair to establish and verify trust as needed. This is similar to the zone control verification techniques used by Microsoft Office 365, Google, and others, and leverages IANA's de-facto control that a requestor demonstrate that they have control of the zone file prior to changes being published in the root zone. This may be an option for sophisticated TLD managers but may be a challenge for smaller or less sophisticated TLD operators.

Recommendations

ICJ does not recommend implementation of a traditional multifactor authentication system for the RZM currently as the costs and complexity do not justify the small to nil increase in overall system security.

That being said, there is a perception issue worth addressing. Multiple TLD operators – including several large, sophisticated operators – perceive the need for multifactor authentication and believe IANA/RZM lack this functionality. These individuals are not considering the multiple layers of protection and the de-facto multifactor requirements for access to the Registry's zone file and to an employee's email account which achieve a level of *multifactor authentication* by definition. ICJ suggests IANA continue communications with TLD managers to remind them that there are multiple levels of authentication and authorization in use as the process is executed.

Finally, ICJ recommends refinement of RZM interactions to eliminate the potential for data leakage that could facilitate social engineering-type attacks. This includes eliminating sensitive content in emails, the use of persistent authentication in HTTPS links, and the availability of ticket information in unauthenticated sessions.

Technical Checks

Issue

Are Technical Checks conducted in an overly burdensome way given their benefits? Can the same stability goals be achieved in some other way?

There is a perceived lack of transparency, consistency, and clarity of purpose in the pre-delegation technical checks. One check in particular – serial number consistency – creates operational challenges for large TLD operators.

Background and Findings

IANA and Verisign perform several technical checks on proposed root zone changes prior to publication. The stated purpose of these checks is to ensure the security and stability of the root zone and to provide a check against the introduction of technical errors.

Several TLD operators noted that these technical checks were opaque (the TLD manager does not know what is being checked or why) and one check in particular – zone file serial number agreement across all authoritative servers – can create delays in the Root Zone Change process by delivering apparently false negative results.

Serial Number Consistency Check

As a requirement prior to implementation of a requested root zone change, IANA checks to ensure that all authoritative DNS servers are advertising the same zone serial number. The intent of this check is to ensure basic hygiene of the authoritative DNS zone: that files are being updated on a timely basis and that the same zone is being published from all authoritative servers. On the surface this is a reasonable check.

However, large TLD operators often leverage large constellations of anycast servers distributed globally. By design, some of these servers serve locations with limited internet connectivity. Laggy or intermittent connectivity combined with a frequently changing zone file result in challenges maintaining serial number consistency across a large constellation of servers.

Lack of serial number synchronization across the entire constellation of servers causes the root zone change process to pause and requires either remediation (a technical check with all serial numbers in agreement), or a manual interaction and exception from IANA. Both TLD operators and IANA report that the exception is often given as the situation is well understood, however, it seems unnecessary and burdensome as manual intervention is required.

One large, sophisticated operator even created a process to stop DNS zone file updates temporarily in advance of requesting zone file changes from IANA. Said differently, this operator changes their normal processes to “work around” this IANA requirement.

TLD managers with whom we spoke recommended a variety of solutions to this problem including: dropping the check altogether; making it a notification only warning as opposed to a blocker in the root zone change process; allowing the operator to specify an allowable “jitter” range in which the error would not be generated; and IANA creating a system to proactively monitor serial numbers and automatically compute an allowable jitter in serial number values.

During discussions, IANA noted that the revision to the RZMS will move away from pass/fail results in favour of pass/warn/fail results. In this revised system, serial number inconsistency would be reported as a warning only and could be acknowledged and skipped by TLD managers, thus not blocking the process. We believe this is a sensible approach.

DNSKEY Present in Parent Zone

Pursuant to IANA technical criteria, “at the time of the listing request there must be a DNSKEY present in the child zone that matches each DS record,” [8] there has been such a requirement since the root zone was signed in 2010.

Several TLD managers noted that this requirement is overly burdensome from a technical perspective, conflicts with their own operational procedures, and/or is not compliant with RFCs. TLD managers have reported that IANA typically does not waive this requirement when requested.

However, the protections offered by the DNSKEY in the child zone prior to publication at the root are powerful. First, it requires the requesting TLD operator to prove they control their zone by publishing the record in advance, which is a significant mitigation against a wide range of intentional and unintentional errors and a fundamental part of the overall integrity of the root zone change process. It also mitigates the risk that the DS record was entered incorrectly – IANA is able to verify the DS is accurate in advance as the DNSKEY is used as a checksum against the DS record. This is not possible absent prepublication of the DNSKEY. This is not a purely theoretical risk: IANA advises that at least twice they waived the requirement, only for the TLD operator to roll their key and then become unresolvable because the DS supplied was wrong (requiring an emergency root zone change to resolve).

[8] https://www.iana.org/help/nameserver-requirements

As with all technical checks, TLD managers can request a waiver for unforeseen and well justified reasons.

Other Technical Checks and Coaching vs. Auditing

While not a widely expressed concern, several TLD operators noted that there is a degree of opacity around the technical checks. They are not sure what is being checked, why, and what is required of them to achieve a passing check. Some expressed annoyance at the whole technical check process (i.e., "I know what I'm doing, leave me alone"). Importantly, we also observed widespread understanding and support that some technical guard rails around the root zone are needed, and that Technical Checks of some type are necessary.

There is a philosophical and historical point worth discussion related to IANA and Verisign's Technical Checks: should these checks be portrayed (and performed) as "audits" enforcing compliance with a set of standards, or as "coaching" in that they are providing helpful assistance and awareness of best practices to TLD operators? Given the critical importance of the global root system, we believe both concepts – enforced compliance with a minimum set of standards supplemented with helpful "coaching" – are appropriate.

ICJ notes that IANA seems to already be moving in this direction with future versions of RZM slated to use a pass/warn/fail approach as opposed to strict pass/fail test. Warnings could be considered "coaching" to provide a heads-up for potential issues, but not blocking the request. Fail would be reserved to establish guard rails for issues that are sufficiently serious. We believe this is a sensible approach.

Currently, IANA/Verisign Technical Checks only occur during a root zone change operation. This is a result of historical practice, but these checks could occur more often as a "health check." While there may have been reluctance in the past for IANA to play such a proactive role, years of mutually cooperative relationship building between TLD operators and IANA have built sufficient trust and public interest in performing these health checks that there are no longer any reasons checks should not be performed more regularly. As discussed previously, IANA must serve a full spectrum of TLD operators ranging from small ccTLD and gTLD operators running only their own domain name registry to large scale commercial operators running potentially hundreds of TLDs or TLDs with millions of registrations. Routine coaching in the form of "health checks" could be a helpful service particularly to the smaller operators.

ICJ notes that DNSSEC, while providing real security benefits, also presents a new and rather obscure set of challenges for TLD operators, particularly smaller ones. For example, algorithm selection, signature expiration, and key rolls, are complex, obscure, and provide opportunity for errors that could take an entire TLD offline. Routine "health checks" providing best practice advice could significantly increase the adoption of DNSSEC by increasing awareness and comfort.

We note that many DNS operators (at all levels of the DNS) use publicly available tools including those available from Verisign[9] and DNS-OARC[10] to perform self-service health checks. It is not difficult to see the value of IANA performing a set of similar checks on a recurring basis as a service to TLD operators. This sort of routine communication, framed as helpful coaching and not a compliance activity, could also be used to create more normalized and frequent communication between IANA and TLD operators, which has other benefits. The interaction could be used to verify contacts and reachability (reducing the "stale" contacts issue), increasing awareness of IANA's "white glove" services, and communication of other "best practice" information that could materially benefit smaller operators.

[9] https://dnssec-debugger.verisignlabs.com/

[10] https://dnsviz.net/

Recommendations and Costs

ICJ does not recommend a change to the requirement that the DNSKEY be present in the child zone prior to updating DNSSEC records at the root. This is a powerful control that mitigates the risk of a variety of intentional and unintentional errors.

ICJ recommends additional documentation and transparency around the Technical Checks being performed by both IANA and Verisign and the success criteria. The costs are the staff time associated with documentation creation and ongoing maintenance and can be measured in tens of hours. The benefit is increased comfort and transparency in this part of the process for the IANA customers and an opportunity for IANA and Verisign to convey the value of these checks to overall internet stability.

In a pass/fail system, ICJ recommends IANA include a hardcoded “allowable jitter” value in the technical check, and work with TLD managers that have previously requested waivers to determine a value that reduces the need for blocking waivers. If it is the case that most operators use increasing serial numbers based on UNIXTIME or some other temporal integer, a small allowable range of acceptable values around the mode serial number (most commonly occurring serial number) should remove the need for waivers while still ensuring that servers are broadly in synch. The cost of this change, again in the tens or low hundreds of hours, can be scheduled in the routine development workflow and will reduce or eliminate the need for manual waivers that are routinely provided. It will reduce the time and cost to the TLD operator of addressing a blocking issue in a change request, evidence goodwill, and remove the need for TLD managers to make operational changes to their systems.

In the contemplated pass/warn/fail revision to RZMS, ICJ supports making serial number inconsistency a non-blocking warning that can be acknowledged and bypassed by TLD operators.

ICJ recommends IANA consider a recurring “health check” service – not tied to root zone change requests – to assist TLD operators (particularly smaller operators) in following best practices. The health check should be offered on an “opt out” basis such that TLD operators that do not wish to participate may choose that option. IANA’s cost would be incurred during upfront design and development phases; the ongoing operational costs should be minimal. The benefits – aside from sharing best practice information with the full range of TLD operators – also include an additional opportunity for IANA to communicate and build relationships with TLD managers. It is easy to see a health check service in conjunction with a contact verification routine which would help address the contact/reachability issue discussed later in this paper. Early detection of stale contacts provides IANA the opportunity to correct and verify contacts during a non-emergency.

API Access for Large Operators

Issue

Would initiation of Root Zone Change requests through an API improve security or save processing resources?

Large TLD operators, perhaps managing hundreds of TLDs, suggested that being able to initiate root zone changes via API (e.g., leveraging EPP) would be helpful. These operators also suggested a simple status report API where they could programmatically monitor pending changes and feed this result into their existing workflow systems.

Discussion

As discussed previously, IANA must serve a full range of customers, from small single ccTLD / gTLD operators to large TLD operators, perhaps managing hundreds of TLDs or millions of domains. During our discussions with managers of large-scale operations, several suggested that submitting root zone requests in a format not requiring initial human interaction in a Web application would improve the reliability and security of the submissions.

ICJ notes that IANA already accepts requests in several formats (e.g., through the RZMS, or by email or fax). Inclusion of an API interface that would collect the same information and initiate the request seems to be the next logical step. There would be no change in the process from that point on. This is purely an intake enhancement. (Implementation of a status monitoring API is more troublesome as that would require mutual authentication and authorization.)

Recommendations

ICJ recommends that IANA investigate a simple API intake, enabling sophisticated TLD operators to initiate a root zone change request programmatically. Customary security controls would need to be in place including protections against flooding, but because the rest of the process is designed to deal with an initial request that is unauthenticated and unauthorized, no additional process changes would be required.

We do not recommend investigating the status API at this point as it is not burdensome (and no TLD operator suggested it was burdensome) for the status to be monitored through the RZMS web application.

Points of Contact

Issue

Is the failure by a TLD manager to keep updated and current Administrative and Technical points of contact a potential single point of failure?

- Should IANA proactively monitor or audit the “contact-ability” of contacts?
- With many TLDs still “new,” should there be increased communication or education concerning this issue?

Background

Each TLD Manager is obligated to maintain up-to-date and accurate Technical and Administrative contacts as part of their root zone file. IANA verifies the ability to communicate with both contacts, and both contacts must approve root zone change requests before they are implemented by IANA.

When the ICJ team set out to survey TLD Managers, it was decided to contact them using the Administrative Contact information listed on the IANA TLD directory page (see, https://www.iana.org/domains/root/db). We made only one contact per TLD to avoid duplicative efforts on the part of TLD Mangers. In addition, different TLDs exhibiting shared email or physical addresses, or a mutual owner were also sent only one notice of the survey.

After sending emails to each TLD Manager, the ICJ team received a number of “bounces.” In total, we received “undeliverable” responses in emails to the Administrative Contact for 29 TLDs.[11]

[11] Examples of error messages received:

xxx@xxx.gov.xx Remote Server returned ‘554 5.0.0 <[0.0.0.0] #5.0.0 smtp; 5.1.0- Unknown address error 550-.. No such user’ (delivery attempts: 0)>’

xxx@xxx.gov.xx Remote Server returned ‘554 5.7.0 < #5.7.520 smtp;550 5.7.520 Access denied, Your organization does not allow external forwarding. Please contact your administrator for further assistance. AS(7555)>’

xxx@xxx.com.xx Remote Server returned ‘554 5.2.2 <DHIEXCH2016-01.xxxxxxxx.com.xx #5.2.2 smtp;554 5.2.2 mailbox full;’

xxx-admin@xxx.xx 550 5.0.350 Remote server returned an error-> 550 Mailbox not found.

websitemanager@xxx.xxx 550 5.1.1 Recipient address rejected: User unknown [this seems to be a whitelist issue and not a bounce]

Findings

The survey results, interviews with individual TLD Managers, and discussions with IANA team members indicated that points of contact are often not maintained in a timely and accurate manner.

- Many TLDs use a generic contact where there is no "one owner" and there is confusion as to who should respond.
- In some TLDs the information has gone stale as staff changes are made.
- In some cases:
    - the contact is a person in a government agency or oversight firm not directly involved with the operation of the ccTLD,
    - personnel exit those posts, and the role is not immediately replaced, or
    - TLD responsibilities are "at the bottom" of that person's list of responsibilities.

In addition, our discussions with registry service (or "backend") providers indicated that TLDs neglecting to keep contacts up to date are often:

- operators of new gTLDs where there are frequent personnel changes, and
- ccTLDs that have infrequent IANA interactions.

During our interviews, we learned of a study where a registry services provider surveyed 209 TLD operators. That interviewee reported that inaccurate contact information was the "biggest problem found." A concern was raised that, in addition to delaying the root zone change request process, inaccurate contact information can present security and stability issues in the event of an emergency.

Discussing these concerns with the IANA Team, we confirmed that IANA had multiple ways to reach TLD operators including a non-published set of contact information. So, while there are some cases where a request might "time out" due to lack of Tech or Admin contact approval, IANA has always been successful in reaching contacts in the cases of required changes or an emergency.

It is also important to note that public contacts serve more than one role, one of which is to be reachable by individuals in the internet eco-system who have a legitimate reason for contacting a TLD for administrative or technical purposes. A second reason is for the purpose of approving RZM change requests. The IANA Team has expressed a desire to work with the community to develop a common set of expectations regarding the purposes of these contacts. The IANA focus to date has been on engineering a solution that separates the public POC role from the authorizer role so that TLD managers can have more flexibility. As the development progresses, it is likely to result in a community engagement on the expectations of these roles.

iana@xxx.gov.xx Remote Server returned '554 5.2.2 <do-mb02.tra.xx #5.2.2 smtp;554 5.2.2 mailbox full;'

dns@xxxxx.xx- ok

xxx.xxx-admin@xxx.x Remote Server returned '554 5.2.1 <aspmx.l.google.com #5.2.1 smtp; 550-5.2.1 The email account that you tried to reach is disabled. Learn more at 550 5.2.1 https://support.google.com/mail/?p=DisabledUser p2si19517165plo.96- gsmtp>'

xx@xxxx.xx Server at DM5PR1701MB1771.namprd17.prod.outlook.com returned '550 5.4.312 Message expired, DNS query failed(ErrorRetry)' Server at xxx.xx (0.0.0.0) returned '450 4.4.312 DNS query failed [Message=ErrorRetry] [LastAttemptedServerName=xxxxx.xx] [DM6NAM11FT035.eop-nam11.prod.protection.outlook.com](ErrorRetry)'

Those TLD operators we interviewed recommended:

- instituting a policy similar to the Whois reminder policy to improve accuracy,
- instituting a more proactive audit with requests for corrective action where the contact proves uncontactable, and
- creating a "role account" for each TLD whose sole purpose is to the IANA point of contact. (That is not to say that the role account cannot have other roles in her/his organization, it is just that one person is designated in each organization as the IANA point of contact).

Recommendation

There are good reasons for maintaining separate Technical and Administrative contacts. When security issues arise, there is an immediate need to reach a technically cognizant individual. Equally compelling is the argument that the Tech contact, while needing to "exist," should not be burdened with every contact as that would detract from accomplishing her/his mission.

In addition, the market has evolved to a place where many TLDs have separate organizations addressing their administrative and technical needs (e.g., employ a registry services provider).

These needs fit well with the IANA requirement for both technical and administrative contacts.

Working with the TLD community, the IANA Team is developing a new model using "authorizers," where the TLD will identify who can approve changes. This could be one or multiple people.

Therefore, and subject to additional consultations among IANA and its customers, the IANA program to develop a model of "authorizers" should continue. In addition:

- The current Tech / Admin contact model should not be replaced by a single "role account."
- Where a TLD has a contracted registry services provider, both IANA contact roles and responsibilities should be described in the contract between the TLD Manager and back-end provider. (This could be a "best practice.")
- IANA could implement an auditing program to improve the chances that the contacts are reachable.
- In cases where there are large time zone differences between IANA staff and the customer, set up (or confirm existing) in-region alternate channels of communication for TLD Managers.

Rationale for this recommendation

- Creating an authorizer role will focus attention on the need to maintain accurate contacts, improve (already good) communications between IANA and its customers, and create flexibility for TLD managers.
- Diversifying contacts within organizations is likely to increase "contactability" and match skill sets to need.
- The Admin and Tech contacts have a public, as well as an IANA, role and so should be maintained.

Cost benefit Analysis / Implications

The recommendations made above are evolutionary in nature, along the lines of a typical continuous improvement program and so would require little additional investment.

A back of the envelope calculation indicates that a contact accuracy auditing program would cost between $20-30K to implement from an accounting standpoint but, given that it can be accomplished with existing staff through a re-prioritization of tasks, the actual incremental cost would be less than that.

IANA Staffing

Issues

Might a lack of staff diversity in training, skill set, experience, or location lead to a single point of failure in any foreseeable scenario?

Do the cumulative staff skill sets and experiences adequately meet the needs of the various types of RZM requests?

Do the staff numbers at each required skill level provide adequate backup in the occasion of unanticipated down-time causing events?

If the answer to the two questions above are yes, are there unneeded redundancies in the staffing?

Background

The organization chart below describes the current IANA staffing.

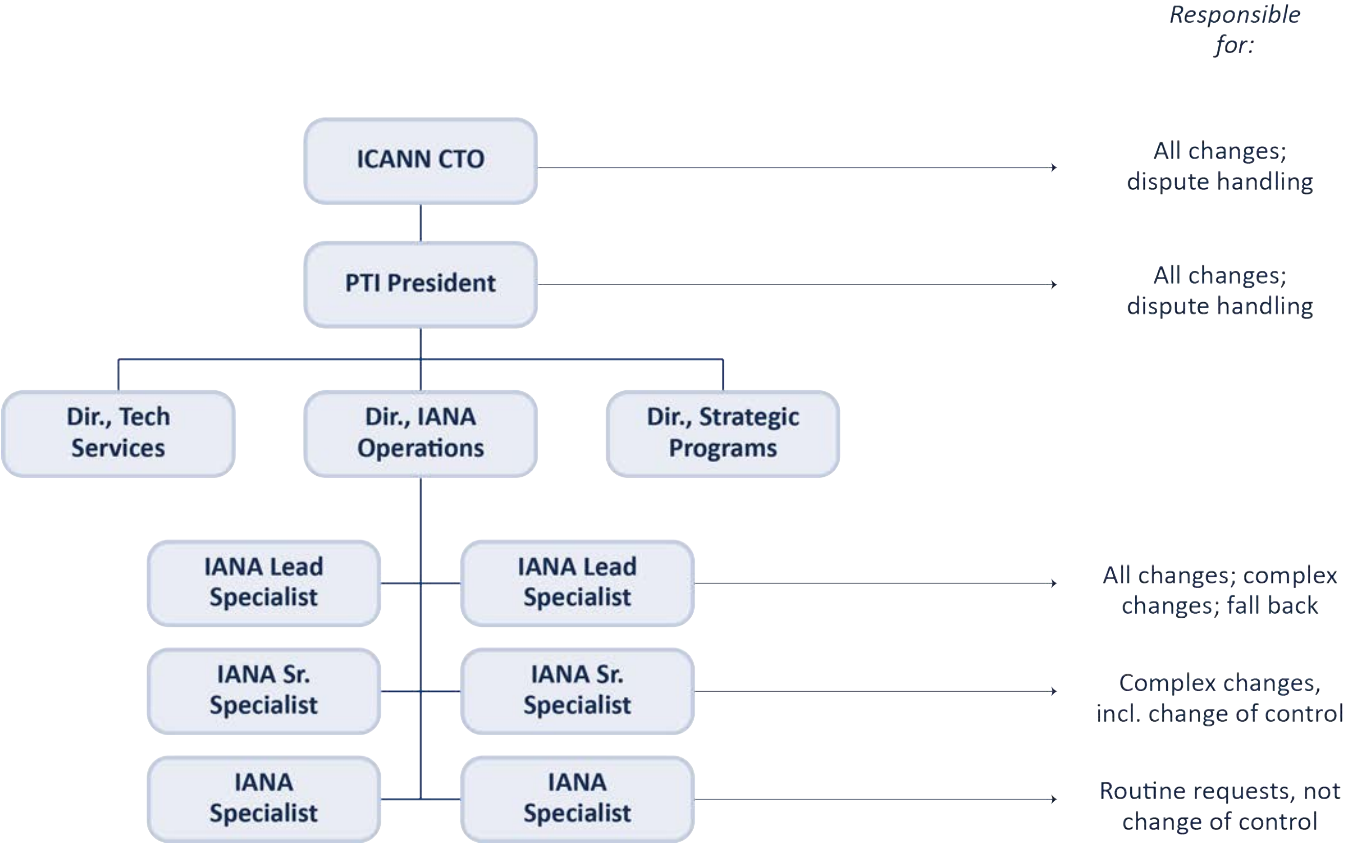


Fig 10. Generic IANA organisation chart

At the time of the study, IANA (PTI) President Kim Davies reported to ICANN CTO, David Conrad. David led IANA prior to his promotion to CTO and can perform any of the tasks in the RZM request process. Kim Davies, with approximately 15 years' experience in IANA can also perform any of the tasks in the RZM process. Both managers have been successful in their IANA roles. This opinion is based on our own study of the IANA operation, reports of the IANA Customer Standing Committee, and the results of our interviews with the IANA team.

By "successful," we mean that IANA response times have improved until they reached an optimum steady state (which has been maintained), CSC reports have been positive without exception, staff levels have increased in numbers and skill set until reaching the planned-for levels, and customer feedback (as described elsewhere in this report) has been positive.

Since this section's original drafting, David Conrad has left his position and has been replaced by CTO John Crain who has similarly deep experience with ICANN and an excellent knowledge of IANA requirements.

Findings

Reporting to Kim Davies are three departments: Technical Services, Strategic Programs, and IANA Operations. This study focuses on the last function. We studied the roles of the first two functions to the extent they support Operations and found that they did not affect the determinations or findings in this report.

Given that TLDs average 1-2 RZM change requests a year, we find that the staff is right sized for the job (with an appropriate cushion for demand variability). Given the survey results that roughly 75% or more requests can be classified as "simple" requests, we find the skill set diversity moderately exceeds the need, which positions the staff well to handle out-of-bandwidth workloads.

Physical diversity: all IANA staff (with one exception who works outside of Operations) reside in California and all but one of those in Southern California. We find this presents a remote but unnecessary risk in the event of natural (or some other) disaster that affects that region of North America.

Related to physical diversity, some respondents to the survey complained that the email life cycle is 24 hours due to time zone differences. After discussion of this issue with IANA staff, examining the processes, and communicating with other customers, we find that time zone differences do not inhibit or delay the performance of the RZM change request process.

Recommendations

We recommend that IANA increase the geographic diversity of its staff to other regions of the United States. This can be done in an evolutionary manner, with new and replacement hires, rather than relocation of existing staff. Alternatively, select ICANN staff can be trained as IANA replacements for the purpose of disaster recovery, but we think this to be a distant "second choice."

Rationale for this recommendation

1. Geographical diversity averts the scenario where infrastructure interruptions (or some types of natural or man-made calamities) effectively bar the entire IANA staff from participating in IANA processes. Recent events in the U.S. state of Texas illustrate risks to even large geographic areas.

2. While there are benefits to co-location, they are easily overcome via online communication platforms to which we have all become accustomed.

3. Nearly all IANA's customers are "remote" regardless of where the IANA staff sits, so there is no other penalty or benefit to co-location from a customer relations standpoint.

4. Training of ICANN staff to sub for IANA staff is a "second choice" because: (1) we think there are considerable benefits in the current staff "co-location" such as team building and ease of information transfer, and (2) non-IANA staff might or might not have the appropriate training for whatever event occurs and might not have the opportunity to develop close team ties that enable rapid communications that are required in an emergency.

Cost-Benefit Analysis

If accomplished in an evolutionary manner, i.e., geographical diversity is increased through attrition or planned staff additions, there is no additional financial cost. ICANN already has geographically distributed offices and has staff working from their home offices.

There are some efficiency costs due to staff separation, but these can be overcome with time and offset by the benefits realised through reduced time zone differences between IANA staff and their customers.

Process Documentation

Issue

Should documentation of IANA processes and sub-processes be augmented to include criteria for decision making and formal memorialization of past decisions on select issues:

- to make inexperienced staff members more independent,
- as a best practice,
- as support for the potential transfer of IANA to a different parent,
- to improve consistency in decision making across the organization.

Background

To document its processes, IANA has created and maintains annotated process flow graphics for every type of RZM process. These include the overall Root Zone Management Change Request Process and its set of subprocess, i.e.,

- The sub-process for receiving and entering (i.e., lodging) the request
- The sub-process of validating the request is well-formed, complete and meets objective assessment criteria (including "Tech Check")
- The sub-process of ensuring proper authorizations are given by designated contacts
- The sub-process to manually review the requested changes to determine if additional information is required
- The sub-process to gather additional information (in the cases of delegation, transfer, or revocation, or where addition information is needed to process the request)
- The sub-process that completes the request, ensuring that new / changed data, reports, and credentials are published into Root Zone file and other appropriate databases

In addition, there are documented processes for

- gTLD Revocation Process
- Emergency Root Zone Change Process

One version of IANA processes documentation is included in the Appendix.

Findings

The process flows are maintained, and all amendments are recorded (substance and date) in the process flow documentation. There is a space for discussion of issues among staff members in the documentation.

The one Root Zone Management Change Request Process and its sub-processes cover all types of root zone changes: e.g., nameserver changes, contact changes, changes of control. Therefore, not every step in each process applies to every type of change. The process documentation makes clear which process segments apply to each type of change. E.g., as a rule, tech checks (embedded in one of the sub-processes) are performed in cases of nameserver and DS record change requests only.

The root zone management system automatically makes the determinations of steps required for each sub-process, so there is no discretion required of the IANA staff.

The process documentation includes the questions that must be satisfied at each step.

There are several instances where there is discretion built into the process depending on information received from the requestor or other circumstances. In certain instances, the process documentation does not provide the criteria by which that discretion is exercised.

1. For example, if the Tech Check step is failed, the step can be by passed if adequate explanation is received by the IANA staff evaluating the change request. However, the documentation does not define criteria for determining the adequacy of the explanation.

2. Similarly, if a change request is for a ccTLD change of control (e.g., a "re-delegation"), the documented process directs IANA Service staff to request "additional information" but does not describe that additional requirement. The IANA services staff is then directed to review the received information and pass the request on to the next step or request additional information if needed.

3. Finally, to complete a change request, the IANA Service staff is required to determine if metadata is needed and, if yes, to add the metadata. In this case the procedure fully describes the criteria triggering the metadata requirement, indicates how (in the IANA Changes Management System) to make that change, and what data ("A-label," "Domain Type," "Status," and "Eligibility") to add.

   Similarly, when determining whether to remove IDN Tables, the staff are instructed to remove the tables only in the case of a "revocation."

   While all documentation is not sufficiently detailed for an unsupervised, inexperienced staff member to complete a change, the documentation in these last two cases do provide clear direction.

During our examination, it was evident that IANA staff members understood the criteria for each decision to be taken in the RZM process and could capably and accurately apply those criteria. In the instances of inexperienced staff, they are always paired with knowledgeable staff or could easily find multiple, knowledgeable staff to provide the appropriate guidance and training. Therefore, we found no risk to the process due to the absence of specific direction, criteria, or prior decisions in the existing documentation.

We also note that the quality and detail of process documentation have steadily improved over the years and understand that, while the NTIA provided oversight, less-detailed documentation was desired for policy reasons. Therefore, we find that the quality of IANA process documentation is improving over time and no adverse event has occurred or is anticipated that would require a change in the current rate of evolution.

Recommendation

We recommend that the documentation of processes and procedures be upgraded to include the criteria for decision making at each step where that decision is not automated by the RM system, and for those where the IANA Services staff can exercise discretion. The documentation should be compliant with NIST business continuity plans or ISO standards for documenting critical processes. IANA might select standards on which to base their documentation model.

The documentation should include a knowledge base of past decisions.

Rationale for this recommendation

1. Best practices for an operation charged with operating DNS-critical infrastructure include that documentation should be designed with the objective that a newcomer or auditor could come to the organization and passably process root zone management changes. We understand that existing, well-designed, right-sized IANA staff redundancies reduce or even eliminate the need for this eventuality, but this type of "documentational completeness" is de rigueur for every critical operation.

2. Well documented processes provide a clear auditable path.

3. Including a knowledge base of common decisions will assist with consistency and reduce controversy in decisions.

Language Services

Issues

Does the English-language requirement present a possible single point of failure in the RZM request process?

Does the English-language requirement dissuade or impair TLD managers from making necessary RZM change requests?

Even if not a single point of failure, would deployment of language services improve IANA service levels as perceived by their customer TLD managers?

Background

IANA requires all TLD managers to communicate in English when dealing with IANA, including Root Zone change requests. There have been no objections to this policy, nor have there been apparent difficulties raised because of the requirement.

When the ICJ team developed questions for the survey of TLD managers, it consulted with the IANA team to ensure the questions were appropriately worded and bounded, and to determine whether the IANA team had any specific requests or advice. The IANA team members recommended that a question be added to test whether TLDs operators needed or wanted to communicate in a language other than English.

The added question read:

English is the required language for IANA official business and correspondence. Is this choice adequate for your needs (check one)?

a) The choice of English is fine.

b) We would prefer to use our commonly used language but can continue to operate using English.

c) The choice of English presents a significant obstacle to our on-going relationship with IANA or deters our efforts to apply for Root Zone Management changes.

Findings

The survey was available in three languages: English, Spanish and Russian. (All recipients of the survey were afforded the opportunity to receive the survey in a language other than English.) Of the 90 survey responses, none called English a significant obstacle to its application for Root Zone Management changes. This indicated that the English-language requirement is not an impediment for access to the root zone change request process, i.e., the English-language requirement is not a single point of failure.

In addition, *all* respondents stated that IANA services were either "fine and staying fine"; or "fine and getting better." Written comments indicated that "fine" reflected genuine approval of the RZM process performance. When combined with other answers, we can infer that language is not a barrier to RZM process participation.

However, 17 TLD managers stated a preference to work in another language. Of those that went on to state a preference:

- Seven requested Spanish
- Two requested French
- One requested Chinese
- One requested Portuguese

Recommendation

While not offering language services at this time, the IANA team should review the survey and interview responses in detail, then collaborate with those TLD Managers that voiced a preference for a language choice. Based on the results of those collaborations, IANA might decide how best to study the potential implementation and consequences of offering language choices in the root zone management change process.

IANA should offer translated documents that describe IANA policies and services. These "peripheral documents" are useful to governments and other policy and oversight bodies that monitor or indirectly benefit from IANA services. Translations of these can facilitate the participation of governments in discussions for improving and using IANA services. Importantly, these peripheral documents are not on the critical path to performing the IANA services themselves. Translation (even efficiently executed) can result in material delays in the RZM change request process. For this reason and because no survey respondents indicated that the English language requirement is a roadblock, we do not recommend that language services be inserted into the change management process itself.

IANA should formalise procedures for "instant" access to language services in the event of an emergency change request where, due to the nature of the emergency, an English speaker is not available. We believe that informal procedures are in place but creating specific written responsibilities will save time in the event of an emergency.

Rationale for this recommendation

- The IANA team included this topic in the survey to determine whether providing language services would facilitate the root zone change request process, to learn more about customer needs.
- Language services might reduce communication barriers and facilitate the accurate execution of root zone change requests somewhat, but the extent of that benefit is not clear given the survey responses. On the other hand, translation services, inserted into a process that is measured in days, not weeks, will likely extend the time for change request processing (and there is the chance for mistranslation of technical documents).
- There is an existing ICANN commitment to translate important documents into other languages that sets a precedent and model for IANA.

- While TLD managers participate in IANA services in English, those in governments and oversight bodies that would benefit from increased knowledge of IANA processes are not part of that communications chain.
- Given the stability / security implications of the RZM process, potential barriers to participation in the process should be given careful consideration; language services in the critical path of RZM change processing might be an expedient or an impediment depending on the situation.

Cost-Benefit Analysis / Implications

Benefit:

Eleven survey respondents indicated a preference for communication in a language other than English, but none indicated that the lack of other-language choice availability was a bar or hindrance to competent participation in the RZM request process. Nothing in our interviews with TLDs managers disturbed this conclusion.

From our perspective, the immediate benefit accruing from providing language services to TLD managers during the RZM process will be in the form of goodwill and a set of informed governmental support teams.

As indicated above, translation of IANA policy and service description documentation can educate those indirectly associated with the IANA RZM services such as governments and other oversight and policy-making bodies.

Cost:

There are several factors contributing to cost uncertainty. Among them are varying expectations of language service requestors, the degree to which IANA can use existing ICANN language service providers, start-up costs such as IANA-process training of language service providers, the administrative costs of operating the program, and the distraction caused by such a program away from IANA's prime objective.

ICANN already competently provides language services that might be shared, so start-up and operating costs are likely to be low, and performance adequate. However, this efficiency might be difficult to realise as the technical language peculiar to TLD managers and the Root Zone Manager are not used in typical ICANN translation exercises.

While initial outlays might be reasonable low, they are likely to grow from requests for a tailored translation protocol per TLD (adding administration costs) and growth in the number of requests. This has been an observable phenomenon across ICANN.

In addition, the provision of language services to the TLDs is likely to give rise to requests from those that could do without it, i.e., TLDs where the translation costs outstrip the benefit. Costs will multiply due to translation requests for correspondence, multiple documents, and standards.

Importantly, the insertion of language services into the RZM change process might result in delays and could also introduce inconsistencies given the technical nature of the information exchanged. These delays might be exacerbated in cases where manual intervention is involved.

Although there might be sound and defensible reasons for drawing a line to provide services only when most meaningful or for a limited type of correspondence, those lines are more difficult to draw than the current bright line of English-language communication. This is the same line ICANN draws in its contracts and accountability frameworks negotiated with TLD managers.

With this, the provision of language services might become an end instead of a means, with KPIs for "number of translations provided" becoming as important as "days to complete requests." This diversion of management attention might distract from performance of the RZM task.

RECOMMENDATIONS SUMMARY

I. Systems & Architecture, we recommend that IANA should:

   a. consider rotating SOC2 auditors during the next cycle

   b. in conjunction with ICANN E&IT, more formally document assumptions and requirements for the custom developed software (specifically RZMS).

   c. establish a lightweight, searchable repository of "case law" to memorialize historical decisions and their rationale.

   d. with ICANN, test security controls, detection, and response capabilities through a targeted offensive exercise program.

II. Authentication:

   a. We do not recommend implementation of a traditional multifactor authentication system for the RZM currently.

   b. The operators that perceive the need for multifactor authentication are not considering the multiple layers of protection and the de-facto multifactor requirements for access to the Registry's zone file and to an employee's email account. We suggest IANA continue communications with TLD managers to gain a common understanding of the multiple levels of authentication and authorization in use as the process is executed.

   c. We recommend refinement of RZM interactions to eliminate the potential for data leakage that could facilitate social engineering-type attacks, including but not limited to: eliminating sensitive content in emails, the use of persistent authentication in HTTPS links, and the availability of ticket information in unauthenticated sessions.

III. Technical Checks

   a. In the contemplated pass/warn/fail revision to RZMS, ICJ supports making serial number inconsistency a non-blocking warning that can be acknowledged and bypassed by TLD operators.

   b. ICJ recommends IANA consider a recurring "health check" service.

IV. Maintenance of Tech and Admin Contacts, we recommend that IANA:

   a. continues to develop a new model using "authorizers," where the TLD will identify who can approve changes. This could be one or multiple people.

   b. continues to maintain Tech and Admin contacts, consider putting into place an auditing plan and improve communications with TLD operators regarding the utility of these contacts.

V. Regarding IANA Staffing: we recommend that IANA increase the geographic diversity of its staff to other regions of the United States.

VI. Process Documentation: We recommend that the documentation of processes and procedures be upgraded to include the criteria for decision making at each step where that decision is not automated (i.e., when the criteria are built into the system), and the IANA Services staff have discretion. The documentation should be compliant with NIST business continuity plans or ISO standards for documenting critical processes.

VII. Provision of Language Services

a. As the IANA team suggested, IANA should offer translated documents that describe IANA policies and services. These “peripheral documents” are useful to governments and other policy and oversight bodies that monitor or indirectly benefit from IANA services. Translations of these can facilitate the participation of governments in discussions for improving and using IANA services.

b. While not offering language services at this time as part of the RZM change process (translation, even efficiently executed, can result in material delays in the RZM change request process), the IANA team should collaborate with those TLD Managers that voiced a preference for a language choice.

c. IANA should formalise procedures for “instant” access to language services in the event of an emergency change request where, due to the nature of the emergency, an English speaker is not available. We believe that informal procedures are in place but creating specific written responsibilities will save time in the event of an emergency.

APPENDIX A: SURVEY RESPONSES

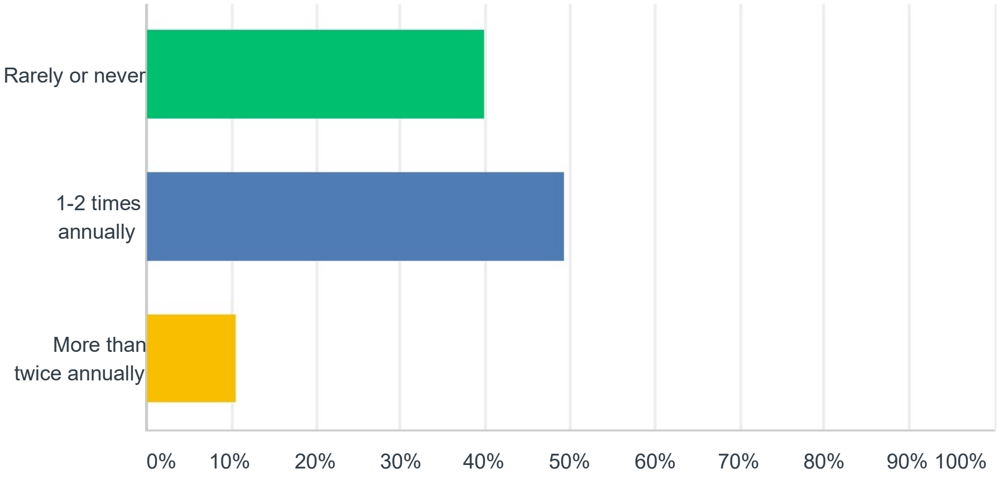
Q1 Which TLD(s) does your firm or entity manage or support? (If multiple TLDs, list one you may list one TLD and include the total number of TLDs under management.)

Answered: 85 Skipped: 0

Details of this response have been redacted by JAS Global Advisors for confidentiality purposes.

Q2 Typically, in one calendar year, each TLD you manage uses the Root Zone Management function (check one):

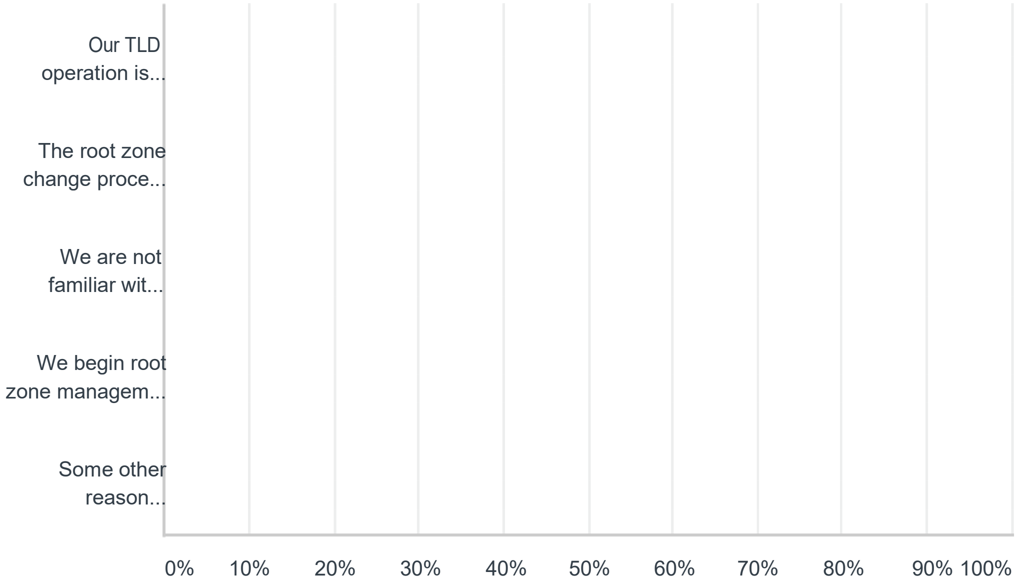
Answered: 85 Skipped: 0



ANSWER CHOICES	RESPONSES	
Rarely or never	40.00%	34
1-2 times annually	49.41%	42
More than twice annually	10.59%	9
TOTAL		85

Q3 If the answer to question (2) is “rarely or never,” was that answer chosen primarily because (select one or more)

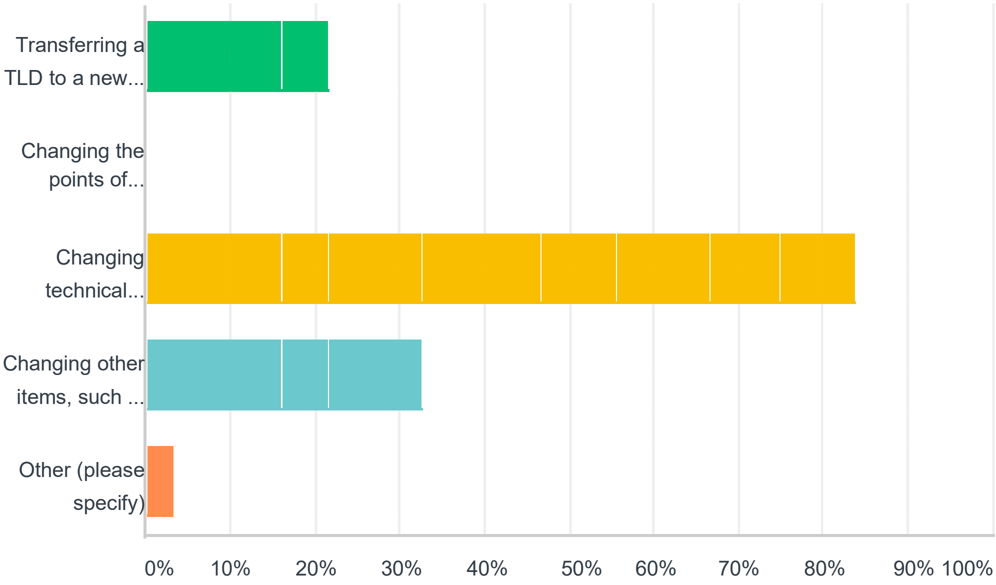
Answered: 41 Skipped: 44



ANSWER CHOICES	RESPONSES	
Our TLD operation is stable, with rare need to request root zone changes	100.00%	41
The root zone change process is too difficult, so we generally attempt to make several changes at one time.	0.00%	0
We are not familiar with the root zone change requirements or procedure	0.00%	0
We begin root zone management changes but frequently withdraw them	0.00%	0
Some other reason described here (fill in the blank):	0.00%	0
Total Respondents: 41		

Q4 Which types of Root Zone Management changes have you requested (check as many as is appropriate):

Answered: 82 Skipped: 3

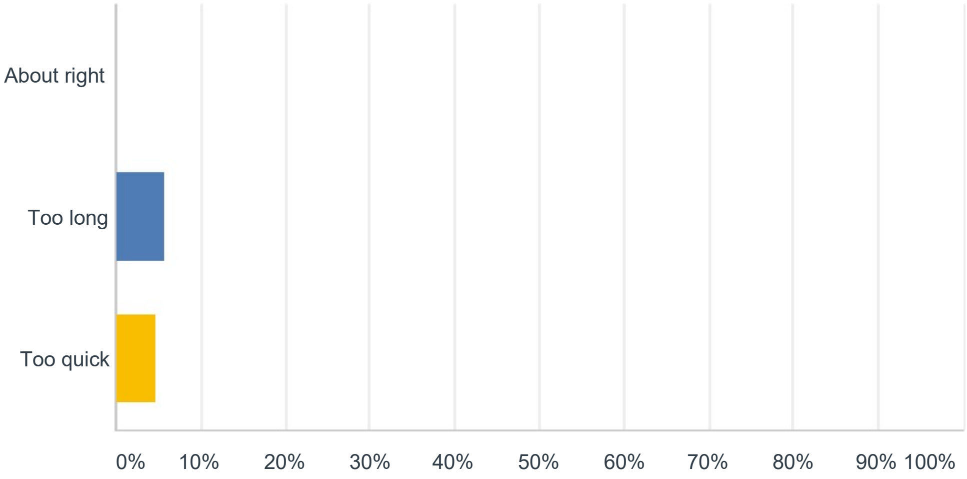


ANSWER CHOICES	RESPONSES	
Transferring a TLD to a new manager	21.95%	18
Changing the points of contact for the TLD	64.63%	53
Changing technical configuration of the domain, such as nameservers and DS records	84.15%	69
Changing other items, such as the WHOIS/RDAP server or the web address	32.93%	27
Other (please specify)	3.66%	3
Total Respondents: 82		

#	OTHER (PLEASE SPECIFY)	DATE
1	Updating IDN tables	4/30/2021 10:16 AM
2	DNSSEC related matters.	4/13/2021 8:29 AM
3	DNSSEC, Root Zone look up and we also refer to the IANA Root Zone web quite frequently.	4/13/2021 6:26 AM

Q5 Typically, the time required for the Root Zone Management process to successfully complete is (check one):

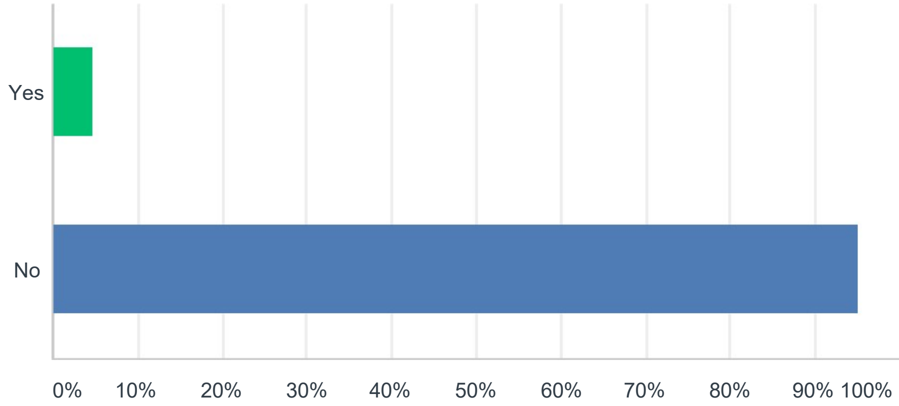
Answered: 84 Skipped: 1



ANSWER CHOICES	RESPONSES	
About right	89.29%	75
Too long	5.95%	5
Too quick	4.76%	4
TOTAL		84

Q6 Are there any steps in the Root Zone Management process that you think are unnecessary or redundant? (check one):

Answered: 83 Skipped: 2

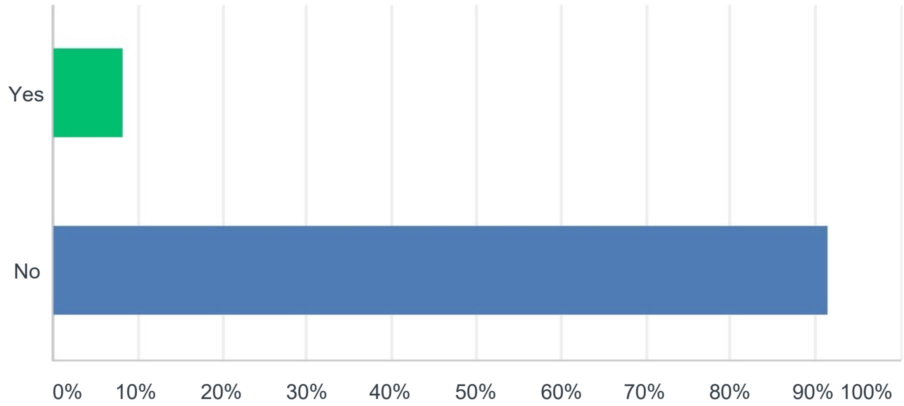


ANSWER CHOICES	RESPONSES	
Yes	4.82%	4
No	95.18%	79
TOTAL		83

#	IF “YES,” OR YOU WISH TO MAKE A COMMENT, PLEASE DESCRIBE THE STEP(S) AND, IF POSSIBLE, STATE WHY THE STEP(S) IS (ARE) UNNECESSARY OR REDUNDANT (FILL IN THE BLANK):	DATE
1	Sometimes it is possible to have different SOA for the zone since our anycast partners may be slow to distribute new zone in timely maner. In that case RZM would detect SOA serial difference and refuse the change, it would be nice that we could override this and post our proposed changes.	4/23/2021 6:06 AM
2	DNSSEC Key Signing Key (KSK) rollover with the Double DS method routinely elevates the process into manual processing; same applies to SOA seriel number discrepancies	4/17/2021 6:36 AM
3	It can be painful when another party uses the same nameserver and needs to vote but doesn't.	4/14/2021 11:16 PM
4	SOA serial consistency check - authoritative nameservers for frequently updated zones will often be out of sync, but this is generally not a serious issue as long as those servers are seeing regular updates. if it doesn't already, this system should also be anycast-aware and check from multiple locations, and use the NSID EDNS option to report which anycast instance(s) have issues.	4/12/2021 1:41 AM
5	But all we have changed for a long time are DNS settings, so we are unaware of the procedures for other changes or how redundant they might be.	4/7/2021 11:04 PM

Q7 Are there any steps in the Root Zone Management process that you think are unnecessarily costly or burdensome for the TLD operator? (check one):

Answered: 84 Skipped: 1

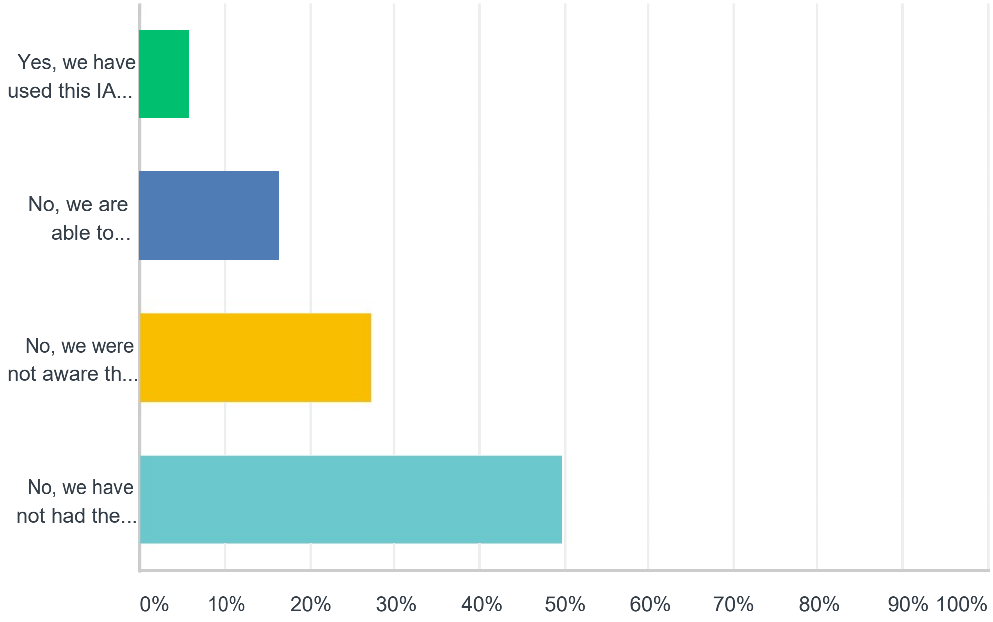


ANSWER CHOICES	RESPONSES	
Yes	8.33%	7
No	91.67%	77
TOTAL		84

#	IF "YES," OR YOU WISH TO MAKE A COMMENT, PLEASE DESCRIBE THE STEP(S) AND, IF POSSIBLE, STATE WHY THE STEP(S) IS (ARE) UNNECESSARILY COSTLY OR BURDENSOME (FILL IN THE BLANK):	DATE
1	Glue Policy described at https://www.iana.org/help/obtaining-consent third paragraph - "Changes that impact multiple domains"	4/27/2021 1:19 PM
2	If changing DNS for a TLD that is used in other TLDs, all contacts are required to allow the change. This creates scalability issues for changing DNS servers in that TLD.	4/19/2021 2:20 PM
3	When technical checks fail (for reasons that can be explained and do not warrant an undue delay in the process), the time to clarify is too long - each email exchange tends to take 24h due to timezones. Note that this comment applies to the process as witnessed on the last technical change request, which has occured at least 1 maybe 2-3 years ago.	4/18/2021 1:48 PM
4	see response to Q6	4/17/2021 6:36 AM
5	The serials across all our nameservers are eventually consistent. Sometimes the RZM health check detects that some serials accross our nameserver are not in sync and stops the change, but the next second they may be back in sync. We have to manually trigger the check again. The healthcheck could be more tolerant or could retry more or both of the latter.	4/14/2021 10:08 AM
6	Currently DS records update are manual form filling and prone to error. A secure automated method is needed.	4/11/2021 9:01 PM
7	My last NS change was held up due to the need to get "DoC signoff" on it. I thought the USG was out of the picture since the transition. I've been meaning to follow up on this with IANA/PTI but it is too far down on my priority list at the moment.	4/8/2021 12:35 PM

Q8 Do you participate in the IANA offer to assist and work closely with TLD operators on the planning, coordination, and implementation of complex requests, (like bulk updates or requests with unique needs)? (check one)

Answered: 84 Skipped: 1

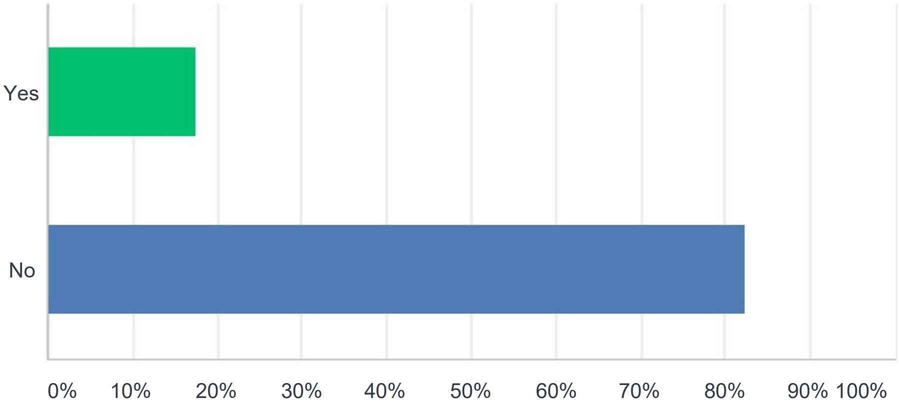


ANSWER CHOICES	RESPONSES	
Yes, we have used this IANA service.	5.95%	5
No, we are able to complete complex requests on our own.	16.67%	14
No, we were not aware that IANA performed this advisory and coordination service.	27.38%	23
No, we have not had the need for such help.	50.00%	42
TOTAL		84

#	WHAT OTHER SERVICES COULD IANA OFFER TO ASSIST TLD MANAGERS IN THE CHANGE REQUEST PROCESS?	DATE
1	Providing the ability to make certain changes without going through the full approval process would be useful. The ability to suppress email notifications where a bulk change is made with the agreement of both parties would be useful.	4/15/2021 9:48 PM
2	Provide emergency technical support, for example when the TLD Operator should immediately update/remove the DS record associated to the TLD zone(s). Also, if the TLD zone is temporarily not operational, allow the TLD operator to use an emergency email address (which should be associated to its contacts), to interact with the IANA Staff. The email address would be created under another extension (.com, .net...)	4/15/2021 7:53 AM
3	beats me?	4/13/2021 6:26 AM
4	DS record validation	4/12/2021 1:41 AM
5	We would like to learn more about this form of assistance.	4/8/2021 1:08 PM

Q9 Do you perceive or believe there are any vulnerabilities or a lack of appropriate security measures in the Root Zone Management process (check one)?

Answered: 85 Skipped: 0



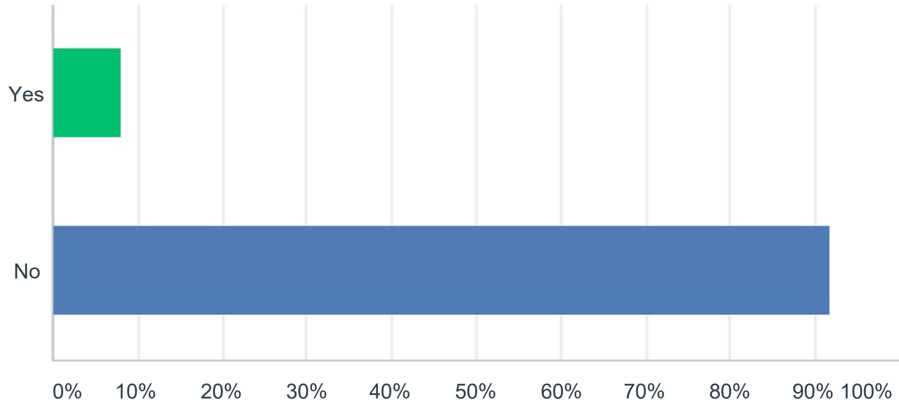
ANSWER CHOICES	RESPONSES	
Yes	17.65%	15
No	82.35%	70
TOTAL		85

#	IF "YES," OR YOU WISH TO MAKE A COMMENT, PLEASE DESCRIBE THE VULNERABILITIES OR LACKING SECURITY MEASURES (FILL IN THE BLANK):	DATE
1	Our DNS engineering manager suggests that RZM access should require multi-factor authentication, including confirmations.	4/30/2021 10:16 AM
2	Although multi-factor authentication would be welcome, all IANA requests need DNS verification steps. So even if RZM is compromised, the security of the DNS infrastructure of the TLD operator will deter some unwelcome changes for TLDs that already DNSSEC-signed.	4/19/2021 2:20 PM
3	the confirmation link for approval of IANA root zone change requests being sent via plain text email (SMTP TLS encryption nonwithstanding) is at least an abstract risk	4/17/2021 6:36 AM
4	May be to add a factor like OKTA Verify to approve or reject changes.	4/16/2021 1:52 PM
5	Login with only username and password is not adequate anymore, as those credentials can be lost easily. Two-factor-authentication should be made a requirement for each account that can change any TLD's data (at least for the transaction). When each and every bank around the world moves to two-factor authentication, it is unclear to me how a cornerstone of the internet infrastructure can live with only username / password. The email verification loop does offset that security risk a bit, though a more sophisticated directed attack could also circumvent that mechanism (by infiltrating the email system of the TLD operator).	4/15/2021 11:29 PM
6	I think having an 'accounts and users' system where a RO or BERO is assigned an account and can create users within it would be helpful to reduce password sharing.	4/15/2021 9:48 PM
7	security settings for account: - 2fa - access for whitelistes ip-addresses	4/15/2021 11:50 AM
8	2 factor authentication on the https://rzm.iana.org/ is missing, as well extended user management (like individual users) and fine-grained permissions management (that particular user may read, modify, delete that particular resource/object style permissions mgmt).	4/14/2021 10:08 AM

9	I think as a recommendation It would be to add two factor authentication to the platform, to provide a bit more security. I do not consider the process related to the zones have vulnerabilities	4/13/2021 2:43 PM
10	I would rather get confirmation request to my primary email address. I believe the secondary email address is for emergency use only.	4/13/2021 12:15 PM
11	We think it would be better to have a double factor authentication for the web page rzm.iana.org	4/13/2021 7:54 AM
12	RZM tool needs MFA!	4/12/2021 2:55 PM
13	2FA on the RZM frontend. PGP signing of email templates.	4/12/2021 1:41 AM
14	User/password authentication could be a security weakness. Even with the approval needed from Admin and Technical contacts for any request. Adding a Second Factor Authentication will be a good step to reinforce security.	4/9/2021 5:12 AM
15	There should be second factor authentication for logging in to root zone management account.	4/9/2021 12:56 AM
16	Have you considered 2FA in admin logins?	4/8/2021 1:08 PM
17	The Root Zone Management System MUST use 2FA. At least offer it as an option as it may not be possible to impose it on a global basis.	4/8/2021 12:35 PM
18	I am not am expert in this area. Have security experts reviewed the processes for vulnerabilities?	4/7/2021 11:04 PM

Q10 Do you perceive or believe there are weak points or single points of failure in the Root Zone Management Process (check one)?

Answered: 85 Skipped: 0

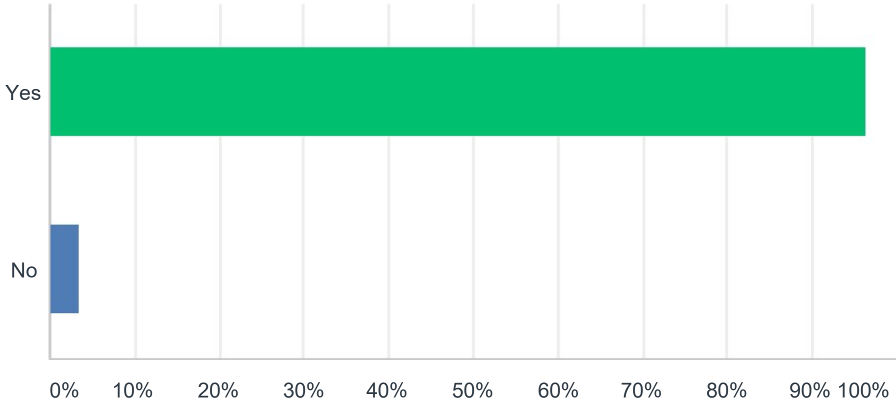


ANSWER CHOICES	RESPONSES	
Yes	8.24%	7
No	91.76%	78
TOTAL		85

#	IF "YES," OR YOU WISH TO MAKE A COMMENT, PLEASE DESCRIBE THE SINGLE POINT(S) OF FAILURE: (FILL IN THE BLANK)	DATE
1	The technical checks are not transparent enough (what is tested, from where (!), what are the detailed results, what would have been expected)	4/18/2021 1:48 PM
2	A change introduced recently, where IANA apparently insists on having a particular person indentified for what otherwise is a role address (admin and tech contact) lacks explanation and the "bigger picture"	4/17/2021 6:36 AM
3	See above, authentication in the web interface. Also, the fact that the rzm.iana.org website is available to the public might expose it to DDoS or similar forms of attack (brute force), though i don't know which types of countermeasures are in place against such attacks.	4/15/2021 11:29 PM
4	It can be painful when another party uses the same nameserver and needs to vote but doesn't. In particular if the update is an emergency one (eg a datacentre has just burnt down) the delay is a problem.	4/14/2021 11:16 PM
5	It's not a major concern, but I'm wondering if IANA staff and RZM on-line system are geographically redundant.	4/14/2021 10:39 PM
6	The single points of failure may lie in the personal nature of the points of contact. It requires careful planning to make an IANA change to make sure the points of contact are available in the time frame the change is running. We have made sure that more people can read the email exchanges between IANA and point of contact to make sure we can react quickly on the emails.	4/9/2021 3:17 AM
7	Unknown. What happens when the site is unavailable? Does IANA have insider risks accounted for?	4/8/2021 1:08 PM
8	See comments for Question 9.	4/8/2021 12:35 PM

Q11 Do the Root Zone management systems and architecture (infrastructure) work smoothly and efficiently for you (check one)?

Answered: 83 Skipped: 2

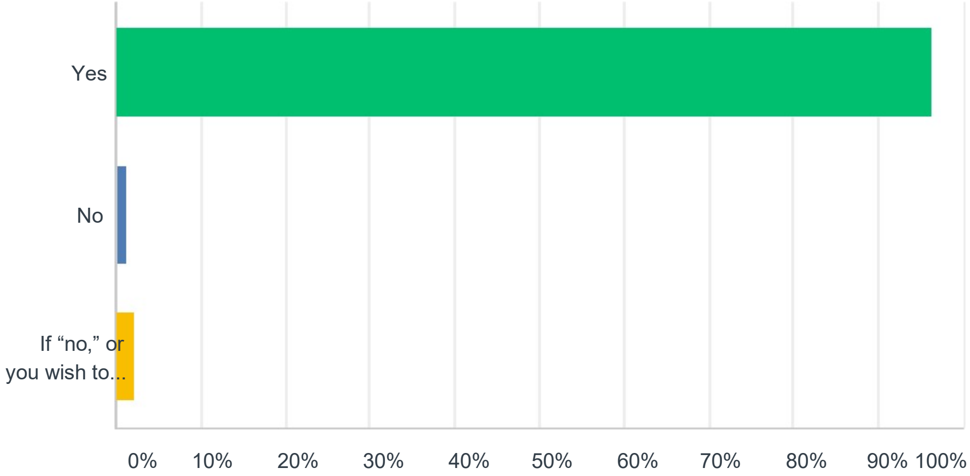


ANSWER CHOICES	RESPONSES	
Yes	96.39%	80
No	3.61%	3
TOTAL		83

#	IF "NO" OR YOU WISH TO MAKE A COMMENT, PLEASE DESCRIBE AREAS WHERE THE SYSTEMS AND ARCHITECTURE (INFRASTRUCTURE) COULD BE IMPROVED (FILL IN THE BLANK):	DATE
1	yes, but please see Q6	4/17/2021 6:36 AM
2	The process does work it is just slow.	4/14/2021 11:16 PM
3	There are times when a request seems to get "stuck" in states like "Pending Zone Testing" for a few days, with no explanation as to what is going on there.	4/12/2021 2:55 PM
4	We would like to have an extra role defined in the IANA process, namely the DNS operations role, who requests a start of a change. This is now done through the e-mail template, which is error-prone because of the nature of this channel.	4/9/2021 3:17 AM
5	We hope so!	4/8/2021 1:08 PM
6	But we do not ask for anything complex.	4/7/2021 11:04 PM

Q12 Do the Root Zone management process systems, business relationships and communications work smoothly and efficiently (check one)?

Answered: 85 Skipped: 0

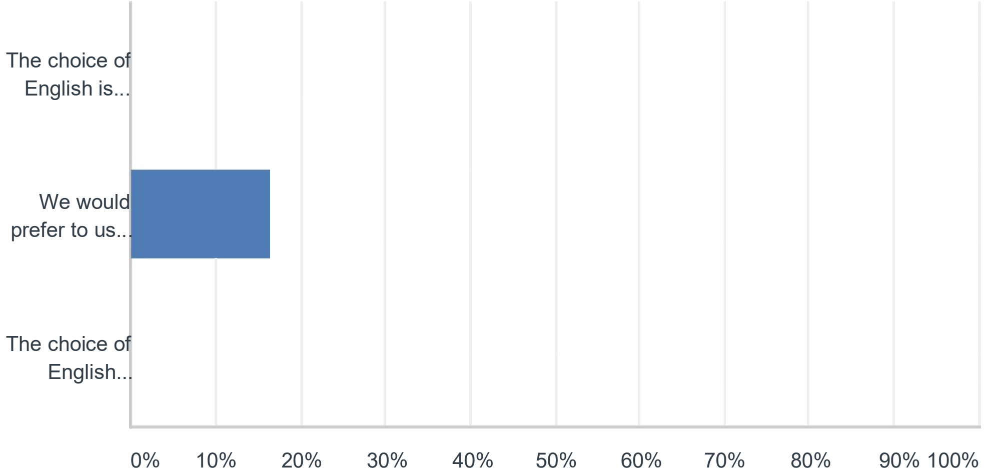


ANSWER CHOICES	RESPONSES	
Yes	96.47%	82
No	1.18%	1
If “no,” or you wish to make a comment, please describe areas where smooth and efficient operating systems could be improved (fill in the blank):	2.35%	2
TOTAL		85

#	IF “NO,” OR YOU WISH TO MAKE A COMMENT, PLEASE DESCRIBE AREAS WHERE SMOOTH AND EFFICIENT OPERATING SYSTEMS COULD BE IMPROVED (FILL IN THE BLANK):	DATE
1	this should not be a yes/no question	4/17/2021 6:36 AM
2	Currently a request may take up to a few days. Please shorten the time to complete them within one day.	4/11/2021 9:01 PM

Q13 English is the required language for IANA / PTI official business and correspondence. Is this choice adequate for your needs (check one)?

Answered: 85 Skipped: 0

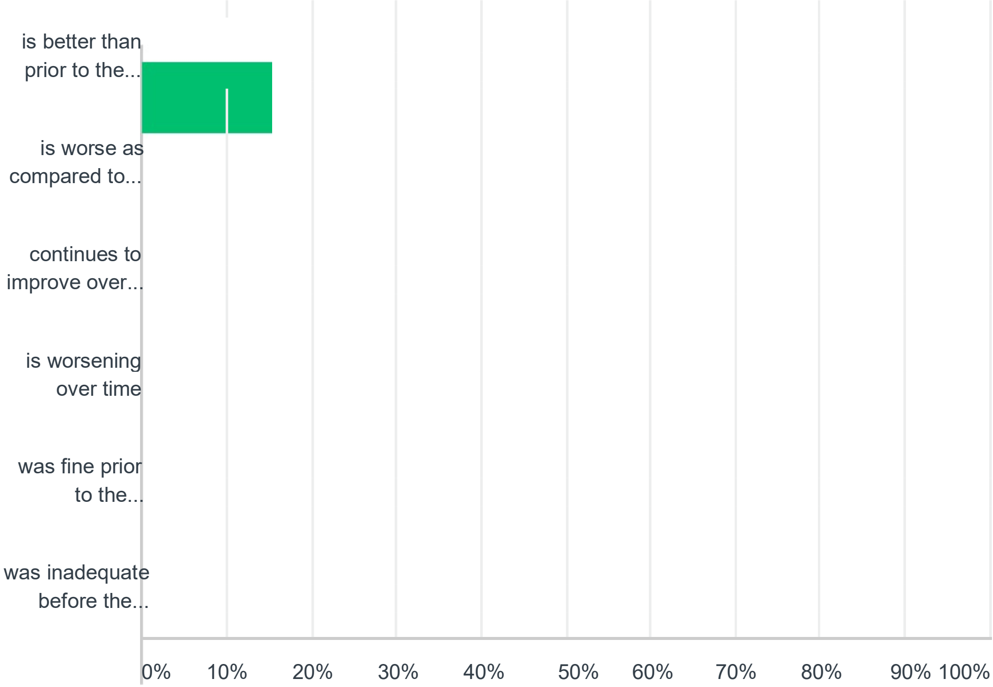


ANSWER CHOICES	RESPONSES	
The choice of English is fine.	83.53%	71
We would prefer to use our commonly used language but can continue to operate using English.	16.47%	14
The choice of English presents a significant obstacle to our on-going relationship with IANA / PTI or deters our efforts to apply for Root Zone Management changes.	0.00%	0
TOTAL		85

#	HAVING CHECKED CHOICE "2" OR "3," THE LANGUAGE OF CHOICE IS (FILL IN THE BLANK):	DATE
1	French	4/15/2021 11:26 AM
2	French	4/15/2021 7:53 AM
3	Chinese	4/14/2021 11:02 PM
4	Spanish	4/13/2021 3:39 PM
5	Spanish	4/13/2021 2:43 PM
6	Spanish	4/13/2021 7:54 AM
7	Spanish	4/12/2021 5:52 AM
8	Spanish	4/9/2021 5:12 AM
9	Portuguese	4/8/2021 5:59 AM

Q14 IANA (now PTI) became independent of the U.S. government in 2016. Since that time, is it your opinion that the performance of the Root Zone Management process (select one or more):

Answered: 84 Skipped: 1



ANSWER CHOICES	RESPONSES	
is better than prior to the transition	15.48%	13
is worse as compared to prior to the transition	0.00%	0
continues to improve over time	34.52%	29
is worsening over time	0.00%	0
was fine prior to the transition and is fine now	50.00%	42
was inadequate before the transition and is inadequate now	0.00%	0
TOTAL		84

#	PLEASE ELABORATE ON THE SELECTIONS ABOVE (FILL IN THE BLANK):	DATE
1	Indeed, we dont enough info to compare bc we are the new manager since [after the transition – the date has been redacted by JAS Global Advisors for confidentiality purposes].	4/27/2021 5:28 AM
2	The only issue we identified is not related to RZM, which is the IDN table management. So this was not covered by the USG contract and was since improved.	4/19/2021 2:20 PM
3	[introduction says 'select one or more' but allows only one] this is hard to tell without going through old interactions; the gutt feeling, if allowed, suggests that technical changes find their way into the root zone a bit quicker than before	4/17/2021 6:36 AM
4	My perception is that transactions are executed more quickly than before (i remember change requests during times of US government shutdown), but that could just be an individual	4/15/2021 11:29 PM

	perception.	
5	We have developed a great working relationship with the IANA team. They are helpful and responsive.	4/15/2021 9:48 PM
6	We think it was fine prior to the transition and is fine now.	4/14/2021 11:02 PM
7	I feel that the time required for implementation of a change has been somewhat reduced.	4/14/2021 10:39 PM
8	From our side of view, Becoming independent is an internal issue	4/13/2021 1:09 AM
9	changes are processed faster as US gov approval is no longer needed	4/12/2021 1:41 AM
10	RZM process is having a steadily evolution since the transition, making the process less burdensome.	4/9/2021 5:12 AM
11	As [the name of the TLD manager has been redacted by JAS Global Advisors for confidentiality purposes] become TLD operator after [the transition – the date has been redacted by JAS Global Advisors for confidentiality purposes], therefore we are not aware of the previous management process of IANA	4/9/2021 12:56 AM
12	The IANA staff has been great, and the overall processing time has been reduced.	4/8/2021 9:51 AM
13	Faster, as there is no need for approval of US DoC.	4/8/2021 7:04 AM
14	We didn't make any requests to you after the transition but we sure it should't be worse than before.	4/8/2021 5:49 AM
15	Did not notice any major change.	4/7/2021 11:04 PM
16	we rarely use PTI service so its hard to tell	4/7/2021 10:37 PM

Q15 Please make any other comments regarding the IANA / PTI Root Zone Management process, including: any aspects that might be improved by either streamlining or added security, areas that require improved documentation, explanation or transparency what you consider to be the most important points described above, and areas of this survey where you feel particularly certain or uncertain of your responses. (fill in the blank):

Answered: 28 Skipped: 57

#	RESPONSES	DATE
1	Nits on the RZM tool function: 1) Sometimes a request enters an 'Exception' state, but no other information is available. 2) When a contact has both a public and private email address, changes in the 'Pending Confirmation' state do now show which of the two addresses - they both can show up as needing confirmations, but you cannot tell which one is which on the page. 3) When changing some "non-standard" items, the description of the change as shown under the 'My Requests' can be incorrect or misleading. 4) A 'Resend confirmation email' button would be very handy! Additional comment from the team (TLD manager's DNS Engineering team; the name of the TLD manager has been redacted by JAS Global Advisors for confidentiality purposes]): "I have always found the team members working with us and responding to our inquiries to be extremely helpful and knowledgeable." and "my experience with IANA / PTI personnel has been absolutely outstanding!"	4/30/2021 10:16 AM
2	I value the stability of the service. However, there is always room for improvement.	4/20/2021 10:08 AM
3	In case of severe problem (such as DNSSEC validation issue), requiring immediate action: Is there an emergency procedure other than email?	4/20/2021 7:17 AM
4	IANA has always responded to our request in a timely manner	4/20/2021 2:34 AM
5	For non-DNSSEC signed TLDs, the single factor authentication can be a risk factor. So while our TLDs are not exposed in that threat vector, not all TLDs are DNSSEC-signed and would be prone to hijack.	4/19/2021 2:20 PM
6	please cf Q6 and Q10; changes to the RZM process shoiuld be layed out in detail and discussed with the relevant community well in advance, as they affect critical infrastructure and TLD internal process, even if those changes do eventually increase the security and stability	4/17/2021 6:36 AM
7	The current process works fine for us.	4/16/2021 1:52 PM
8	As noted above an account/user model similar to the NSp would stop password sharing. It would be great if the Root Zone Database not only listed Technical and Administrative Contacts but also a Support Contact. The Root Zone Database should list A Labels and U Labels.	4/15/2021 9:48 PM
9	Maybe an FAQ could be interesting and/or some additional ressources about changes that are within the scope of the IANA/ITP RZM and the processes to be followed. Resources in languages other than English could also be an interesting point to consider.	4/15/2021 11:26 AM
10	for a single brand TLD the chances are that the brand business owner would expect their registry front end provider to deal with the majority of the IANA tasks that come along from time to time. Some of the questions possibly require perhaps a n/a choice beside the yes and no responses	4/15/2021 9:09 AM
11	Improve on the time zone for e-mail responses so that IANA queries and/or responses are within the working hours of the requester to avoid long interaction and process delays	4/15/2021 6:20 AM
12	We think all aspects are all right for us.	4/14/2021 11:02 PM

13	1) Regarding question (13), although I've never had a problem with conversations in English, I expect they are written in clear and concise language. 2) While it's before the transition to PTI, I have a little concern on the estimated first response time of the emergency contact procedure. In [a year before the transition, the date has been redacted by JAS Global Advisors for confidentiality purposes], we needed an emergency contact with IANA to withdraw a change request. We called 24x7 emergency call center. We didn't got called back for over two hours. We got a contact to an IANA staff directly out of the formal procedure afterwards.	4/14/2021 10:39 PM
14	I would prefer 2fa for accessing RZM.	4/13/2021 12:15 PM
15	IANA/PTI service is good enough and always confident and reliable.	4/13/2021 8:29 AM
16	We were happy with IANA and didn't see the need to change.	4/13/2021 6:26 AM
17	No comments	4/13/2021 5:36 AM
18	provide support number(s) for emergency or holiday periods to handle any unprecedented occurrence.	4/13/2021 12:34 AM
19	RST seems to be a bit prone to errors, which can delay the migration of TLDs from another operator.	4/12/2021 2:55 PM
20	N/A	4/12/2021 1:19 PM
21	I think IANA needs to be Multilingual instead of using English as the official language for communications, specially must use Spanish.	4/12/2021 5:52 AM
22	I have no comments at this moment in time.	4/12/2021 5:09 AM
23	You're doing a great job. Many thanks.	4/12/2021 2:46 AM
24	As stated earlier, it is beneficial to have a third role in the IANA process, namely the requestor of the change. This is mostly a technical role, and one that tracks the change and makes sure the change goes as smoothly as possible. Not only on the side of IANA, but also internal in the organisation.	4/9/2021 3:17 AM
25	we are not very familiar with IANA root management Infrastructure, operations and systems. So it will be helpful if information/documentation is available on IANA website	4/9/2021 12:56 AM
26	The PTI Board should be making final decisions on issues, not the ICANN Board. The ICANN Board should only step in where there is a dispute over a decision made by PTI, as an Appeals mechanism	4/8/2021 3:53 PM
27	The handling of out-of-band requests might need some tweaking. I think there ought to be a way to classify the severity of the out-of-band request to the person who answers the phone on behalf of IANA/PTI so that if, for example, the situation is a ccTLD that has gone dark sparks a near immediate response from whomever is on call for IANA/PTI at that moment, whereas if its only a partial stability issue (for example, one NS has gone dark, but the rest are operational), it could be assigned a lower priority level. This idea is something that IANA/PTI might wish to explore with the Community to sort out a path forward if they wish to explore this idea.	4/8/2021 12:35 PM
28	Your requirements are reasonable. Processing time is quite acceptable. So everything is quite fine. Thank you for you kind service.	4/8/2021 5:49 AM

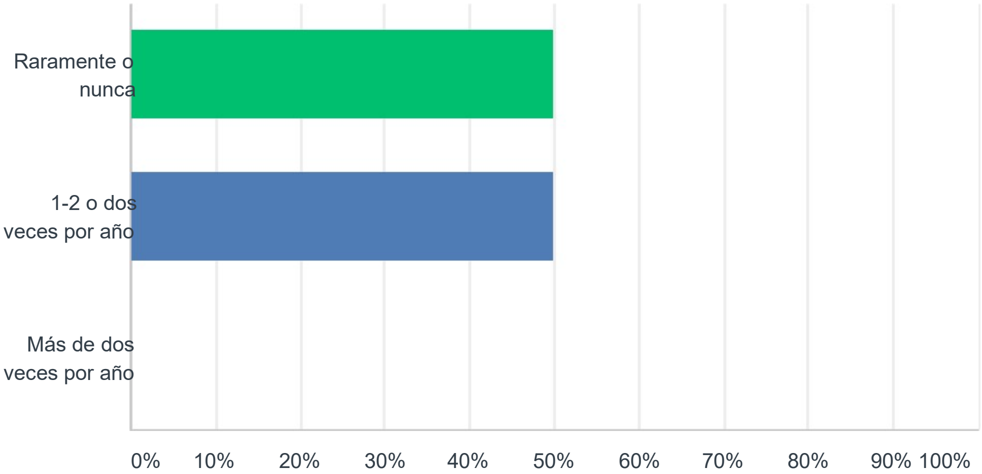
Q1 ¿Qué TLD gestiona o apoya su empresa o entidad? (Si hay varios TLD, enumere uno de ellos e incluya el número total de TLD que gestiona).

Answered: 4 Skipped: 0

Details of this response have been redacted by JAS Global Advisors for confidentiality purposes

Q2 Normalmente, en un año calendario, cada TLD que gestiona utiliza la función de gestión de la zona raíz (marque una):

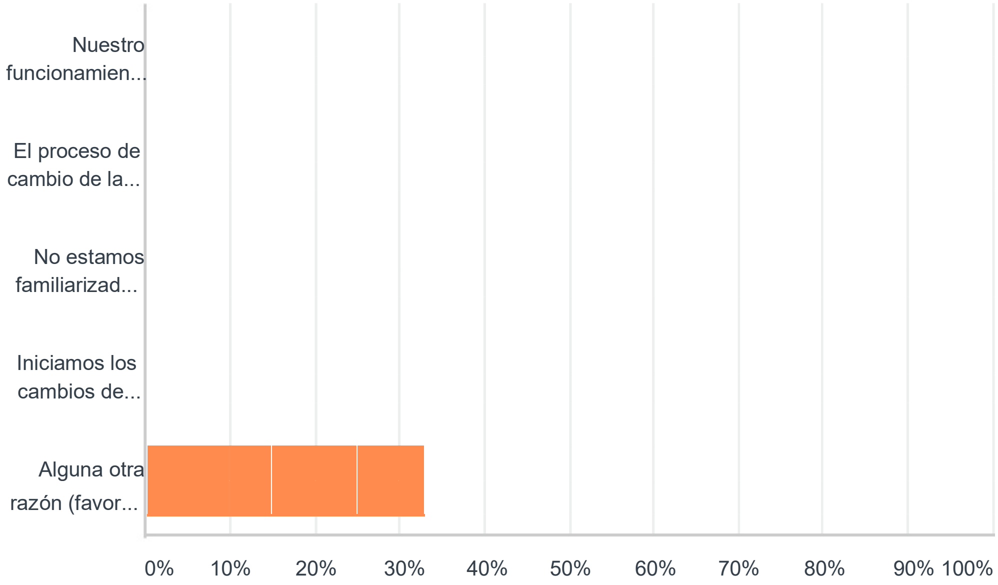
Answered: 4 Skipped: 0



ANSWER CHOICES	RESPONSES	
Raramente o nunca	50.00%	2
1-2 o dos veces por año	50.00%	2
Más de dos veces por año	0.00%	0
TOTAL		4

Q3 Si la respuesta a la pregunta (2) es "rara vez o nunca", ¿se eligió esa respuesta principalmente porque (seleccione una o más):

Answered: 3 Skipped: 1

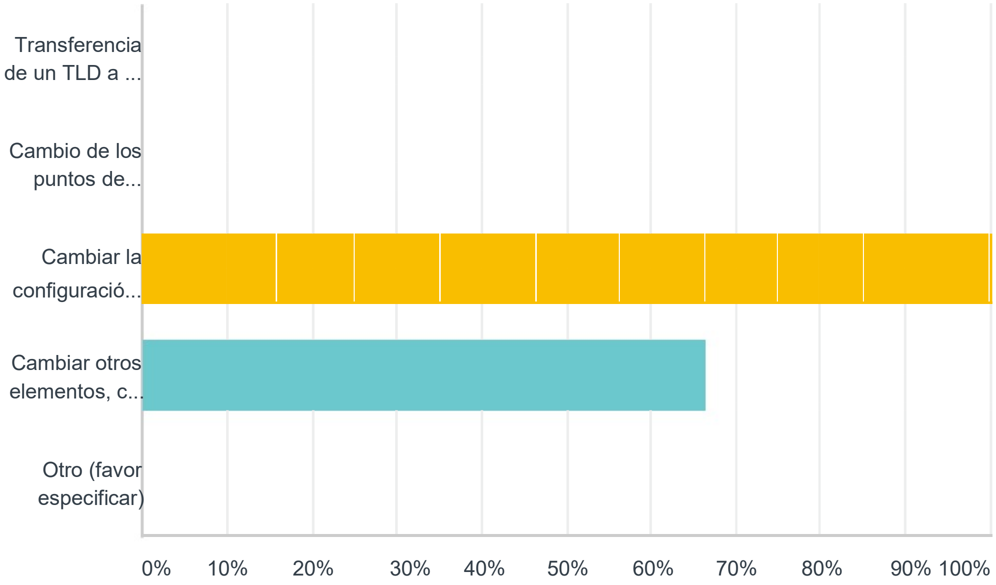


ANSWER CHOICES	RESPONSES	
Nuestro funcionamiento del TLD es estable, y rara vez es necesario solicitar cambios en la zona raíz	100.00%	3
El proceso de cambio de la Zona Raíz es demasiado difícil, por lo que generalmente intentamos hacer varios cambios a la vez.	0.00%	0
No estamos familiarizados con los requisitos o el procedimiento de cambio de la Zona Raíz.	0.00%	0
Iniciamos los cambios de gestión de la Zona de las Raíz, pero los retiramos con frecuencia	0.00%	0
Alguna otra razón (favor describir aquí)	33.33%	1
Total Respondents: 3		

#	ALGUNA OTRA RAZÓN (FAVOR DESCRIBIR AQUÍ)	DATE
1	Este proceso lo genera nuestro RSP [name of the TLD Manager has been redacted by JAS Global Advisors for confidentiality purposes].	4/23/2021 9:21 AM

Q4 ¿Qué tipos de cambios en la gestión de la Zona Raíz ha solicitado? (marque todos los que sean apropiados):

Answered: 3 Skipped: 1

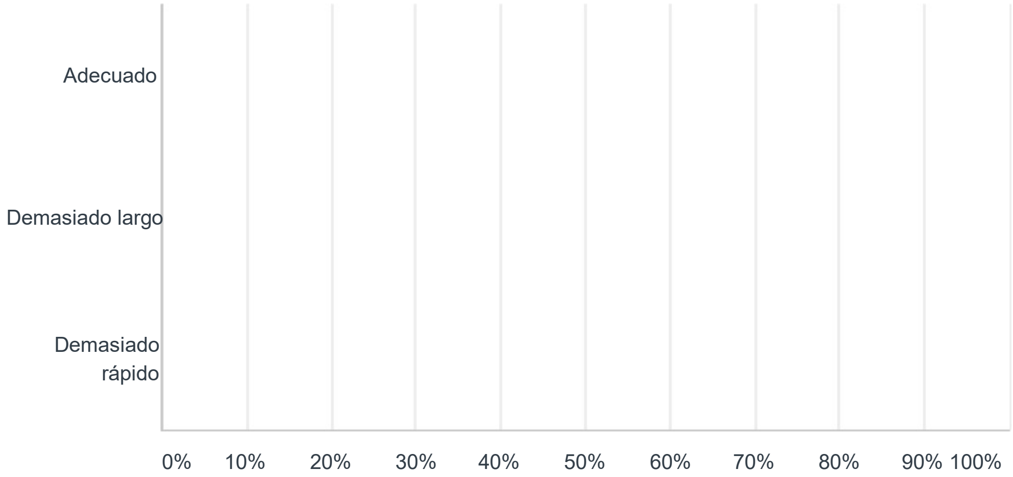


ANSWER CHOICES	RESPONSES	
Transferencia de un TLD a un nuevo gestor	0.00%	0
Cambio de los puntos de contacto del TLD	66.67%	2
Cambiar la configuración técnica del dominio, como los servidores de nombres y los registros DS	100.00%	3
Cambiar otros elementos, como el servidor WHOIS/RDAP o la dirección web	66.67%	2
Otro (favor especificar)	0.00%	0
Total Respondents: 3		

#	OTRO (FAVOR ESPECIFICAR)	DATE
	There are no responses.	

Q5 Normalmente, el tiempo necesario para que el proceso de gestión de la zona raíz se complete con éxito es (marque una):

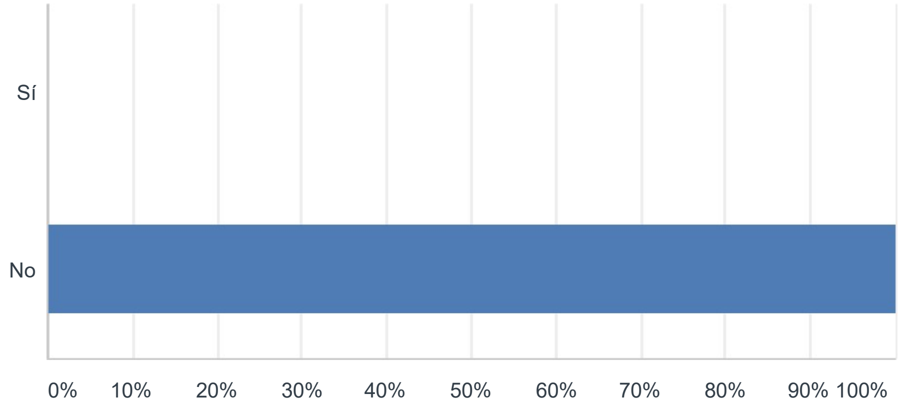
Answered: 4 Skipped: 0



ANSWER CHOICES	RESPONSES	
Adecuado	100.00%	4
Demasiado largo	0.00%	0
Demasiado rápido	0.00%	0
TOTAL		4

Q6 ¿Hay algún paso en el proceso de gestión de la Zona Raíz que considere innecesario o redundante? (marque una):

Answered: 4 Skipped: 0

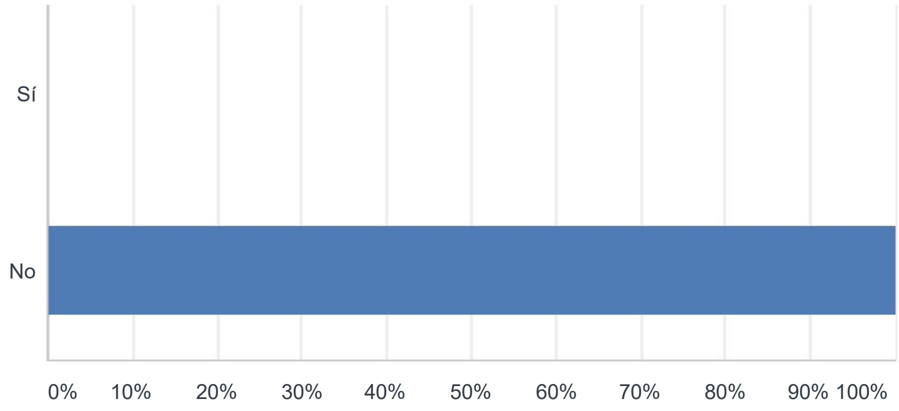


ANSWER CHOICES	RESPONSES	
Sí	0.00%	0
No	100.00%	4
TOTAL		4

#	SI LA RESPUESTA ES "SÍ", O SI DESEA HACER UN COMENTARIO, DESCRIBA LA(S) ETAPA(S) Y, SI ES POSIBLE, INDIQUE POR QUÉ LA(S) ETAPA(S) ES(SON) INNECESARIA(S) O REDUNDANTE(S) (RELLENE EL ESPACIO EN BLANCO):	DATE
	There are no responses.	

Q7 ¿Hay algún paso en el proceso de gestión de la Zona Raíz que considere innecesariamente costoso o difícil para el operador de TLD? (marque una):

Answered: 4 Skipped: 0

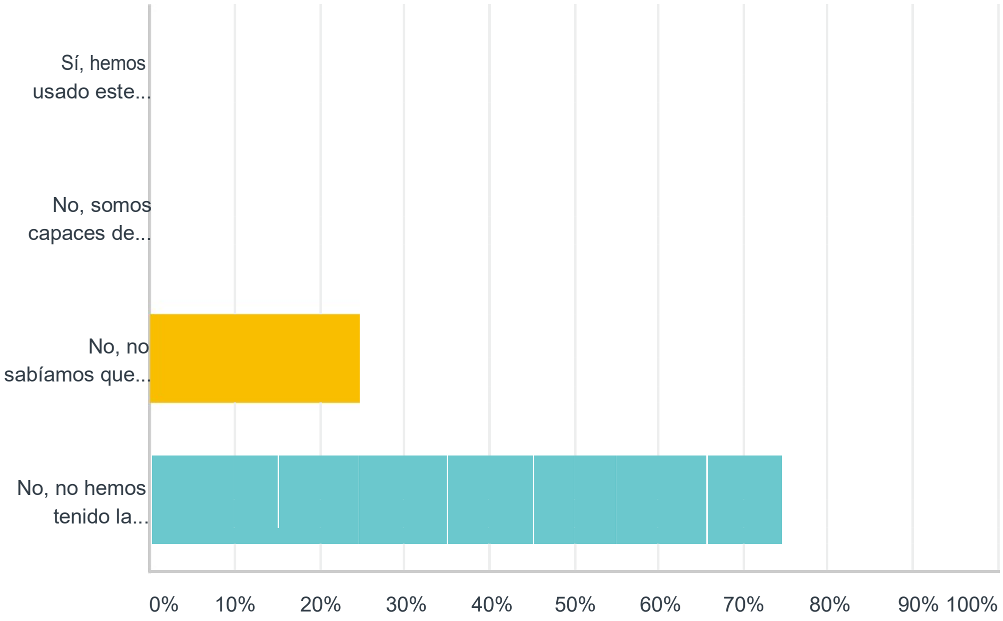


ANSWER CHOICES	RESPONSES	
Sí	0.00%	0
No	100.00%	4
TOTAL		4

#	SI LA RESPUESTA ES "SÍ", O SI DESEA HACER UN COMENTARIO, DESCRIBA LA(S) ETAPA(S) Y, SI ES POSIBLE, INDIQUE POR QUÉ LA(S) ETAPA(S) ES(SON) INNECESARIAMENTE COSTOSA(S) O DIFICULTOSA(S) (RELLENE EL ESPACIO EN BLANCO):	DATE
	There are no responses.	

Q8 ¿Participa de la oferta de la IANA para ayudar y trabajar estrechamente con los operadores de TLD en la planificación, coordinación e implementación de solicitudes complejas, (como actualizaciones masivas o solicitudes con necesidades únicas)? (marque una)

Answered: 4 Skipped: 0

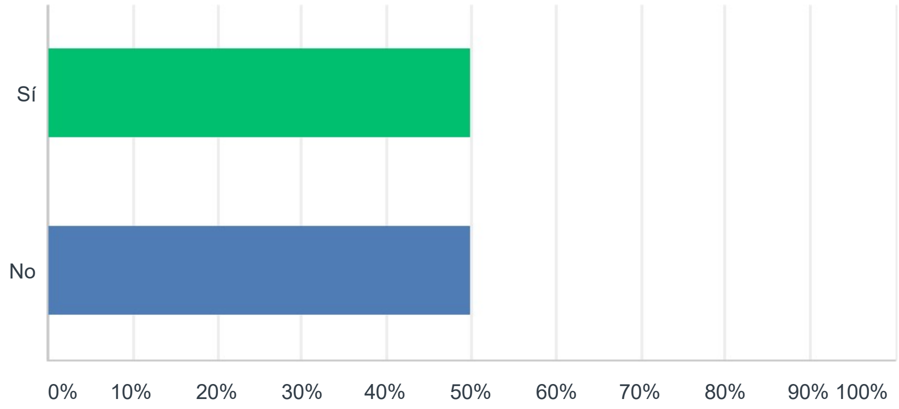


ANSWER CHOICES	RESPONSES	
Sí, hemos usado este servicio de la IANA	0.00%	0
No, somos capaces de resolver solicitudes complejas por nuestra cuenta.	0.00%	0
No, no sabíamos que IANA realizara este servicio de asesoramiento y coordinación.	25.00%	1
No, no hemos tenido la necesidad de esa ayuda.	75.00%	3
TOTAL		4

#	¿QUÉ OTROS SERVICIOS PODRÍA OFRECER LA IANA PARA AYUDAR A LOS ADMINISTRADORES DE TLD EN EL PROCESO DE SOLICITUD DE CAMBIO?	DATE
	There are no responses.	

Q9 ¿Percibe o cree que hay alguna vulnerabilidad o falta de medidas de seguridad adecuadas en el proceso de gestión de la zona raíz? (marque una)

Answered: 4 Skipped: 0

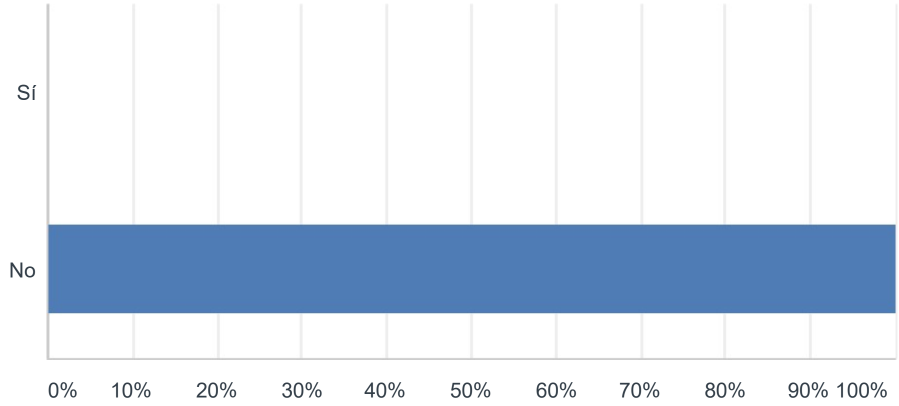


ANSWER CHOICES	RESPONSES	
Sí	50.00%	2
No	50.00%	2
TOTAL		4

#	SI LA RESPUESTA ES "SÍ" O DESEA HACER UN COMENTARIO, DESCRIBA LAS VULNERABILIDADES O LA FALTA DE MEDIDAS DE SEGURIDAD (RELLENE EL ESPACIO EN BLANCO):	DATE
1	El acceso al panel de control debería contar con una opción de autenticación de doble factor o token.	4/13/2021 10:01 PM
2	Agregar un captcha al login	4/13/2021 7:09 PM

Q10 ¿Percibe o cree que hay puntos débiles o puntos únicos de fallo en el Proceso de Gestión de la Zona Raíz (marque uno)?

Answered: 4 Skipped: 0

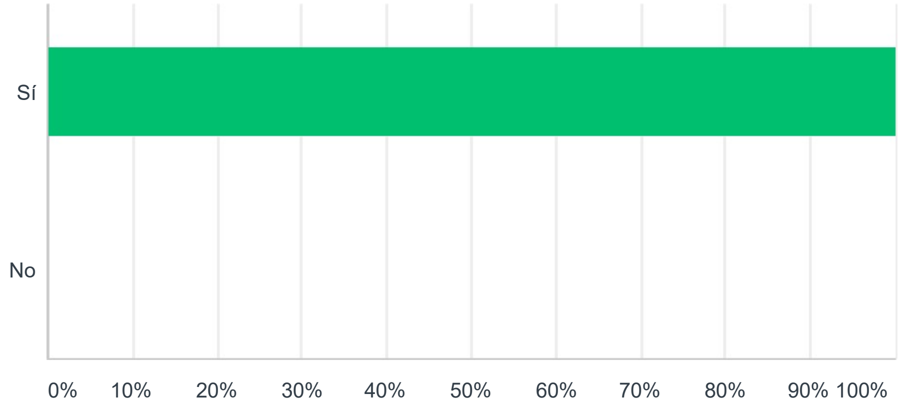


ANSWER CHOICES	RESPONSES	
Sí	0.00%	0
No	100.00%	4
TOTAL		4

#	SI LA RESPUESTA ES "SÍ", O SI DESEA HACER UN COMENTARIO, DESCRIBA EL PUNTO O LOS PUNTOS ÚNICOS DE FALLO: (RELLENE EL ESPACIO EN BLANCO)	DATE
	There are no responses.	

Q11 ¿Los sistemas de gestión de la Zona Raíz y la arquitectura (infraestructura) le funcionan sin problemas y con eficacia? (marque una)

Answered: 4 Skipped: 0

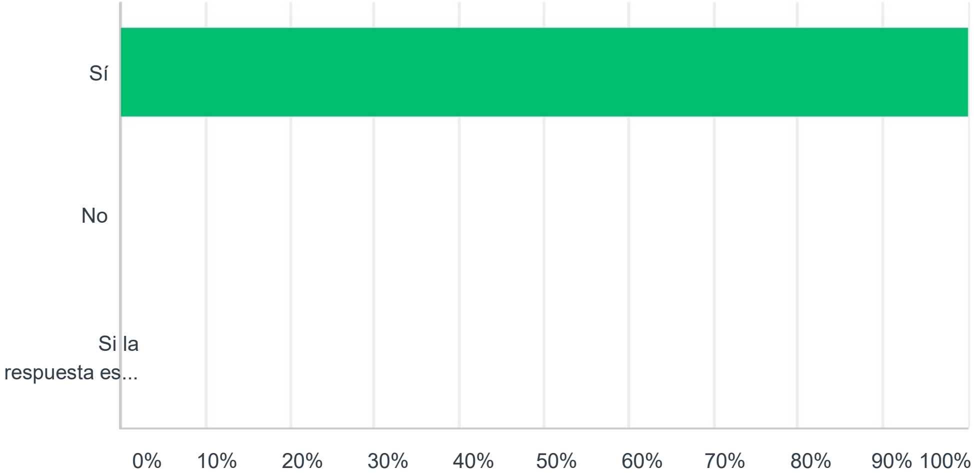


ANSWER CHOICES	RESPONSES	
Sí	100.00%	4
No	0.00%	0
TOTAL		4

#	SI LA RESPUESTA ES "NO" O DESEA HACER UN COMENTARIO, DESCRIBA LAS ÁREAS EN LAS QUE LOS SISTEMAS Y LA ARQUITECTURA (INFRAESTRUCTURA) PODRÍAN MEJORARSE (RELLENE EL ESPACIO EN BLANCO):	DATE
	There are no responses.	

Q12 ¿Funcionan los sistemas del proceso de gestión de la Zona Raíz, las relaciones comerciales y las comunicaciones de forma fluida y eficaz? (marque una)

Answered: 4 Skipped: 0

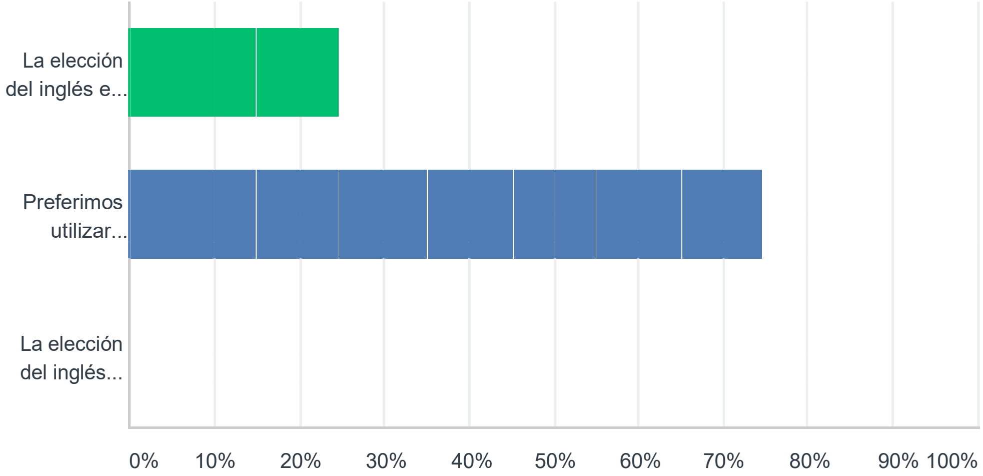


ANSWER CHOICES	RESPONSES	
Sí	100.00%	4
No	0.00%	0
Si la respuesta es "no", o si desea hacer algún comentario, describa las áreas en las que se podrían mejorar los sistemas de funcionamiento fluido y eficiente (rellene el espacio en blanco):	0.00%	0
TOTAL		4

#	SI LA RESPUESTA ES "NO", O SI DESEA HACER ALGÚN COMENTARIO, DESCRIBA LAS ÁREAS EN LAS QUE SE PODRÍAN MEJORAR LOS SISTEMAS DE FUNCIONAMIENTO FLUIDO Y EFICIENTE (RELLENE EL ESPACIO EN BLANCO):	DATE
	There are no responses.	

Q13 El inglés es el idioma requerido para los asuntos oficiales y la correspondencia de la IANA / PTI. ¿Es esta opción adecuada para sus necesidades? (marque una)

Answered: 4 Skipped: 0

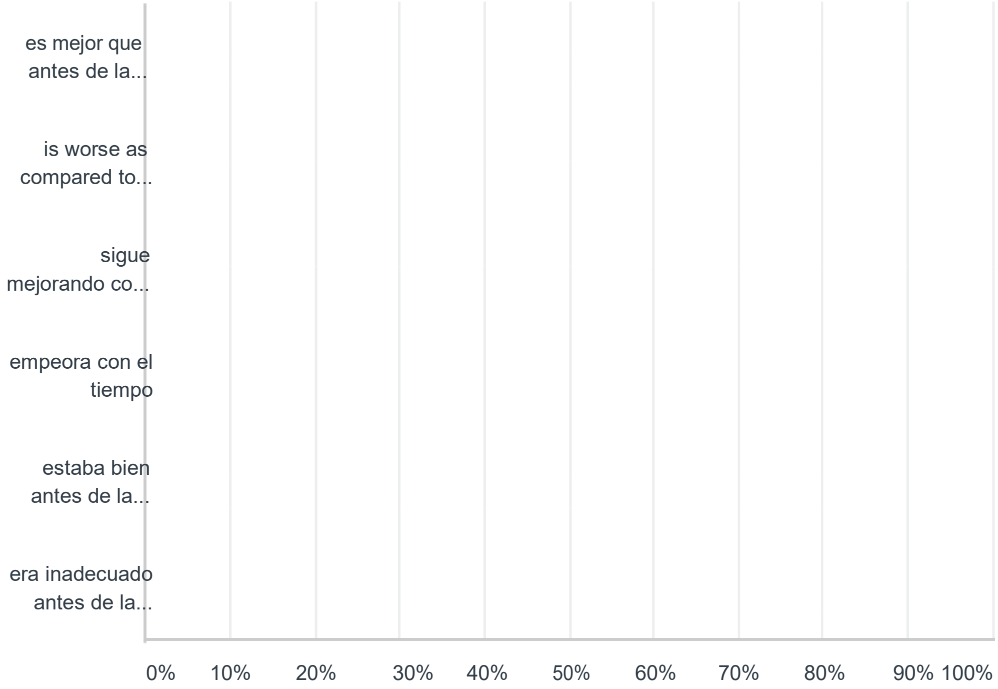


ANSWER CHOICES	RESPONSES	
La elección del inglés está bien.	25.00%	1
Preferimos utilizar nuestra lengua de uso común, pero podemos seguir operando en inglés.	75.00%	3
La elección del inglés supone un obstáculo importante para nuestra relación actual con IANA / PTI o disuade nuestros esfuerzos para solicitar cambios en la gestión de la Zona Raíz.	0.00%	0
TOTAL		4

#	UNA VEZ MARCADA LA OPCIÓN "2" O "3", LA LENGUA ELEGIDA ES (RELLENAR EL ESPACIO EN BLANCO):	DATE
1	español	4/13/2021 10:01 PM
2	español	4/13/2021 7:09 PM

Q14 La IANA (ahora PTI) se independizó del gobierno de Estados Unidos en 2016. Desde entonces, ¿opina que el rendimiento del proceso de gestión de la Zona Raíz (seleccione uno o más):

Answered: 4 Skipped: 0



ANSWER CHOICES	RESPONSES	
es mejor que antes de la transición	25.00%	1
is worse as compared to prior to the transition	0.00%	0
sigue mejorando con el tiempo	50.00%	2
empeora con el tiempo	0.00%	0
estaba bien antes de la transición y está bien ahora	25.00%	1
era inadecuado antes de la transición y es inadecuado ahora	0.00%	0
TOTAL		4

#	POR FAVOR, EXPLIQUE LAS SELECCIONES ANTERIORES (RELLENE EL ESPACIO EN BLANCO):	DATE
1	han mejorado los tiempos de respuesta	4/14/2021 6:36 AM
2	la atención de las solicitudes actualmente es más veloz.	4/13/2021 10:01 PM
3	A mejorado en los tiempos de validación y respuesta. Y debe seguir mejorando y agregando algoritmos para la firma con dnssec	4/13/2021 7:09 PM

Q15 Por favor, haga cualquier otro comentario sobre el proceso de gestión de la zona raíz de la IANA / PTI, incluyendo: cualquier aspecto que pueda mejorarse mediante la racionalización o el aumento de la seguridad; áreas que requieran una mejor documentación, explicación o transparencia; lo que considera que son los puntos más importantes descritos anteriormente; y las áreas de esta encuesta en las que se siente especialmente seguro o inseguro de sus respuestas (rellene el espacio en blanco):

Answered: 1 Skipped: 3

#	RESPONSES	DATE
1	Agregar el algoritmo Ed25519	4/13/2021 7:09 PM

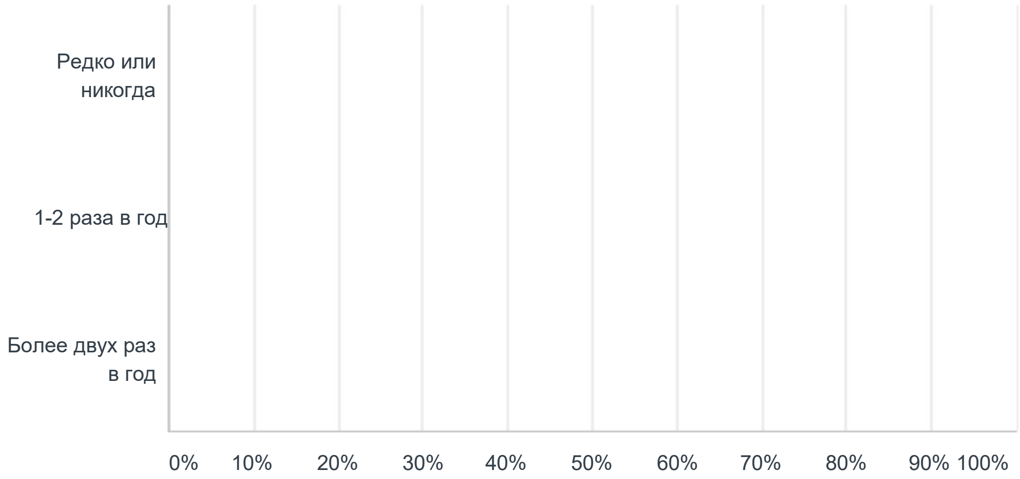
Q1 Какие Домены верхнего уровня (TLD) находятся в управлении вашей организации или поддерживаются ею? (Если таких TLD несколько, вы можете указать один домен и написать общее количество доменов верхнего уровня в вашем управлении). Заполните поле

Answered: 1 Skipped: 0

Подробности этого ответа анонимны JAS Global Advisors. / Details of this response have been redacted by JAS Global Advisors for confidentiality purposes.

Q2 Обычно в течение одного календарного года каждый управляемый вами TLD использует функцию управления корневой зоной (отметьте один вариант):

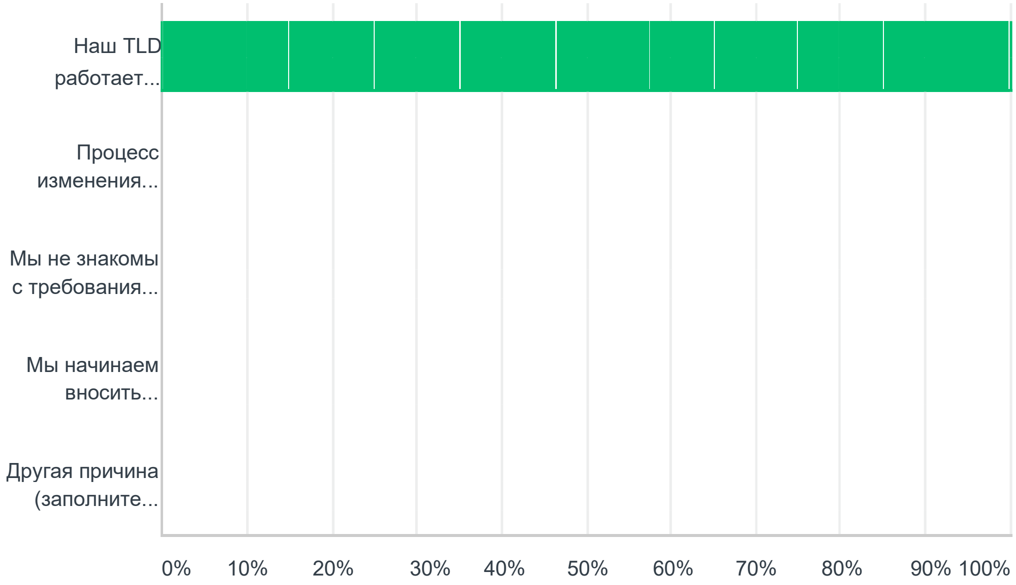
Answered: 1 Skipped: 0



ANSWER CHOICES	RESPONSES	
Редко или никогда	0.00%	0
1-2 раза в год	100.00%	1
Более двух раз в год	0.00%	0
TOTAL		1

Q3 Если ваш ответ на вопрос (2) «редко или никогда», то выберите один или несколько дополнительных пунктов из следующих:

Answered: 1 Skipped: 0

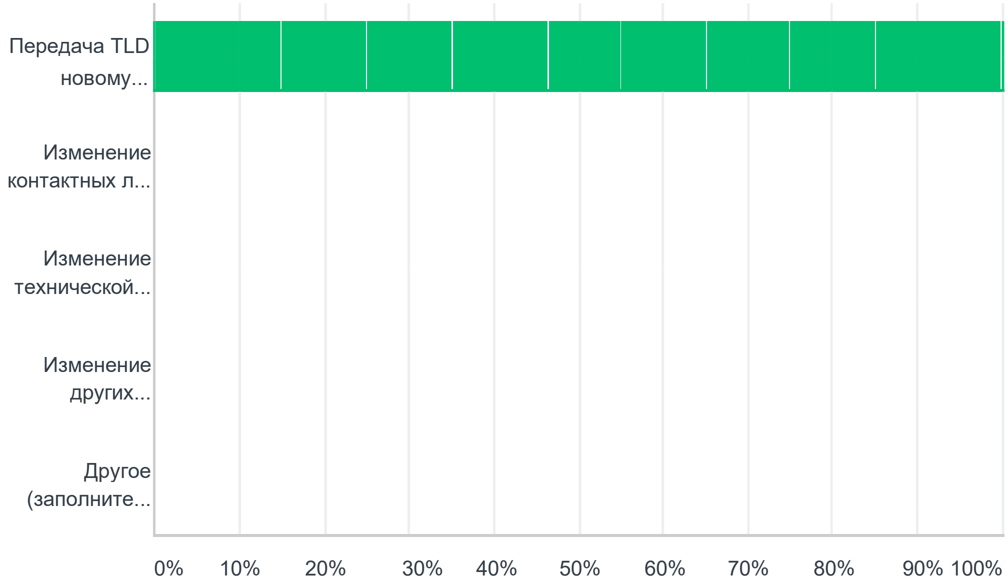


ANSWER CHOICES	RESPONSES	
Наш TLD работает стабильно, запросы на изменение корневой зоны возникают редко.	100.00%	1
Процесс изменения корневой зоны слишком сложен, поэтому мы обычно пытаемся внести несколько изменений одновременно.	0.00%	0
Мы не знакомы с требованиями или процедурой изменения корневой зоны.	0.00%	0
Мы начинаем вносить изменения в управление корневой зоной, но часто отменяем их.	0.00%	0
Другая причина (заполните поле):	100.00%	1
Total Respondents: 1		

#	ДРУГАЯ ПРИЧИНА (ЗАПОЛНИТЕ ПОЛЕ):	DATE
1	мы вносим изменения, только если это требуется	4/29/2021 1:59 AM

Q4 Какие типы изменений в управлении корневой зоной вы запрашивали (отметьте столько, сколько необходимо):

Answered: 1 Skipped: 0

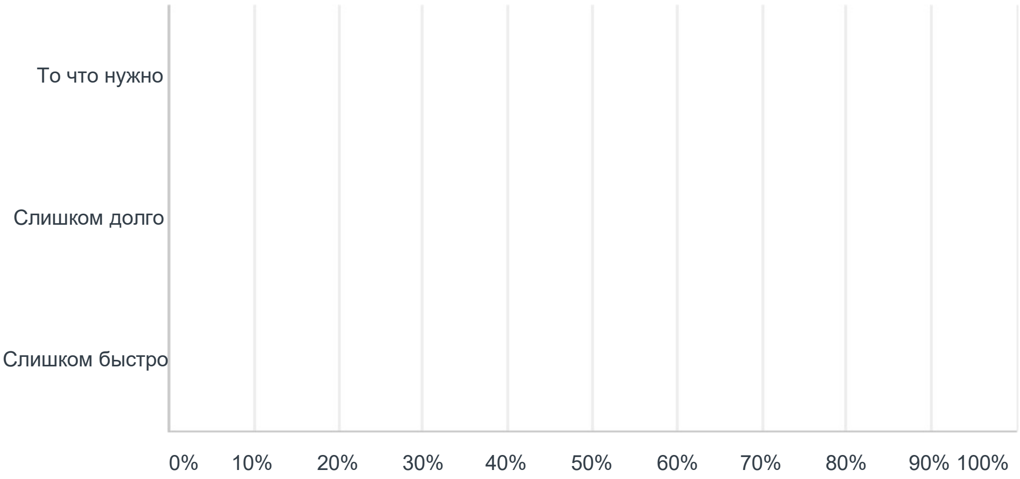


ANSWER CHOICES	RESPONSES	
Передача TLD новому управляющему	100.00%	1
Изменение контактных лиц TLD	100.00%	1
Изменение технической конфигурации домена, например серверов имен и записей DS	100.00%	1
Изменение других элементов, таких как сервер WHOIS / RDAP или веб-адрес	0.00%	0
Другое (заполните поле)	0.00%	0
Total Respondents: 1		

#	ДРУГОЕ (ЗАПОЛНИТЕ ПОЛЕ)	DATE
	There are no responses.	

Q5 Как вы оцениваете скорость выполнения изменений (время, необходимое для успешного завершения процесса управления корневой зоной) (отметьте один вариант):

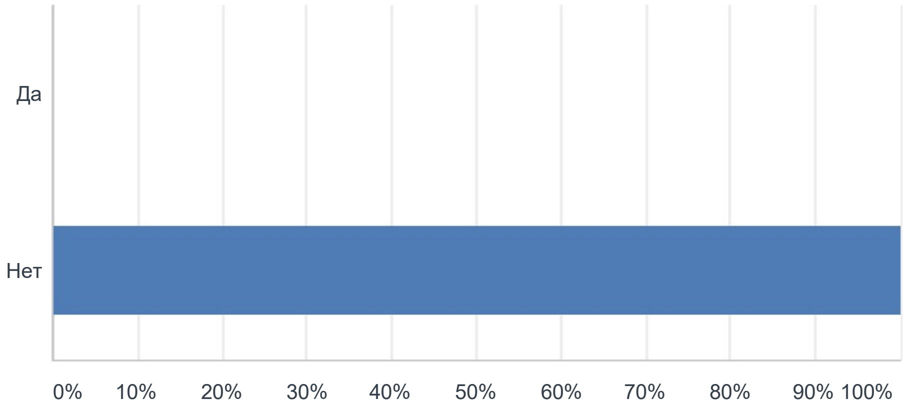
Answered: 1 Skipped: 0



ANSWER CHOICES	RESPONSES	
То что нужно	100.00%	1
Слишком долго	0.00%	0
Слишком быстро	0.00%	0
TOTAL		1

Q6 Есть ли какие-либо шаги в процессе управления корневой зоной, которые вы считаете ненужными или избыточными? (отметьте галочкой один вариант):

Answered: 1 Skipped: 0

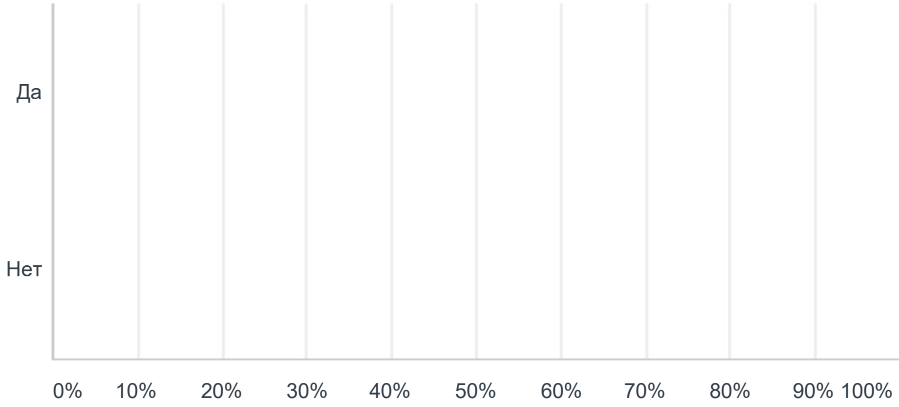


ANSWER CHOICES	RESPONSES	
Да	0.00%	0
Нет	100.00%	1
TOTAL		1

#	ЕСЛИ «ДА» ИЛИ ВЫ ХОТИТЕ СДЕЛАТЬ КОММЕНТАРИЙ, ОПИШИТЕ ШАГ (ШАГИ) И, ЕСЛИ ВОЗМОЖНО, УКАЖИТЕ, ПОЧЕМУ ЭТОТ ШАГ(И) ЯВЛЯЕТСЯ НЕНУЖНЫМ (И/ ИЛИ) ИЗБЫТОЧНЫМ (ЗАПОЛНИТЕ ПОЛЕ):	DATE
	There are no responses.	

Q7 Есть ли какие-либо шаги в процессе управления корневой зоной, которые, по вашему мнению, являются излишне дорогостоящими или обременительными для оператора ДВУ? (отметьте галочкой один вариант):

Answered: 1 Skipped: 0

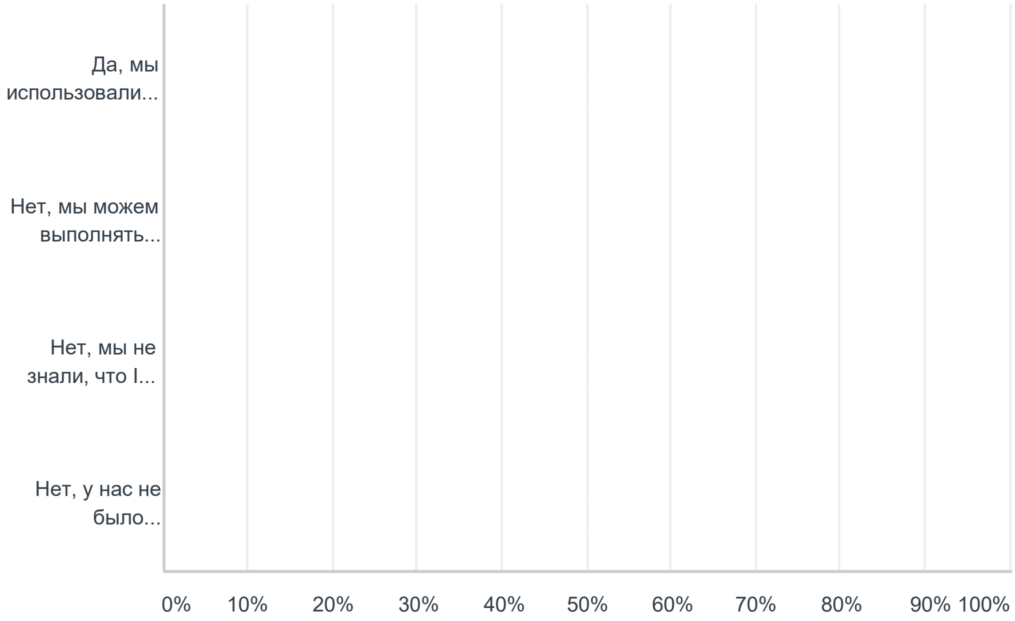


ANSWER CHOICES	RESPONSES	
Да	0.00%	0
Нет	100.00%	1
TOTAL		1

#	ЕСЛИ «ДА» ИЛИ ВЫ ХОТИТЕ СДЕЛАТЬ КОММЕНТАРИЙ, ОПИШИТЕ ЭТАП(Ы) И, ЕСЛИ ВОЗМОЖНО, УКАЖИТЕ, ПОЧЕМУ ЭТОТ(ТИ) ШАГ(И) ЯВЛЯЕТСЯ (ЯВЛЯЮТСЯ) ИЗЛИШНЕ ДОРОГОСТОЯЩИМИ ИЛИ ОБРЕМЕНИТЕЛЬНЫМИ (ЗАПОЛНИТЕ БЛАНК):	DATE
	There are no responses.	

Q8 Участвуете ли вы в предложении IANA о содействии и тесном сотрудничестве с операторами TLD по планированию, координации и реализации сложных запросов (например, множественных обновлений или запросов с уникальными требованиями)? (отметьте один из вариантов)

Answered: 1 Skipped: 0

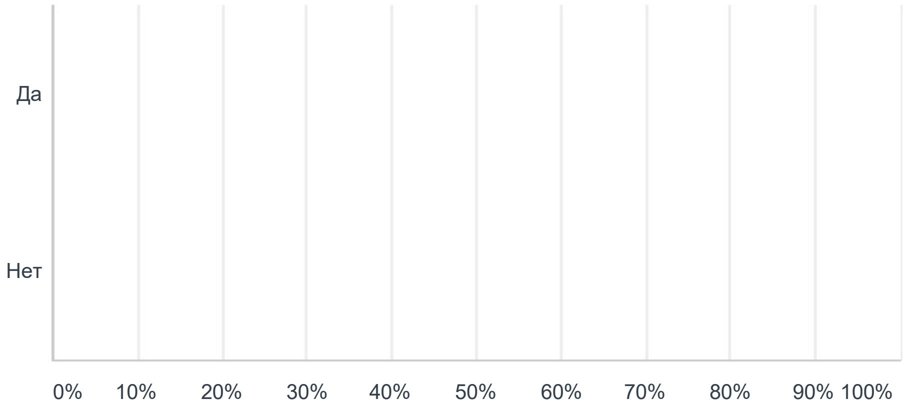


ANSWER CHOICES	RESPONSES	
Да, мы использовали эту службу IANA.	0.00%	0
Нет, мы можем выполнять сложные запросы самостоятельно.	100.00%	1
Нет, мы не знали, что IANA выполняла эту консультационную и координационную услугу.	0.00%	0
Нет, у нас не было необходимости в такой помощи.	0.00%	0
TOTAL		1

#	КАКИЕ ЕЩЕ УСЛУГИ IANA МОЖЕТ ПРЕДЛОЖИТЬ МЕНЕДЖЕРАМ TLD В ПРОЦЕССЕ ЗАПРОСА НА ИЗМЕНЕНИЕ (ЗАПОЛНИТЕ ПОЛЕ)?	DATE
	There are no responses.	

Q9 Считаете ли вы, что в процессе управления корневой зоной есть какие-либо уязвимости или отсутствие соответствующих мер безопасности (отметьте одно из них)?

Answered: 1 Skipped: 0

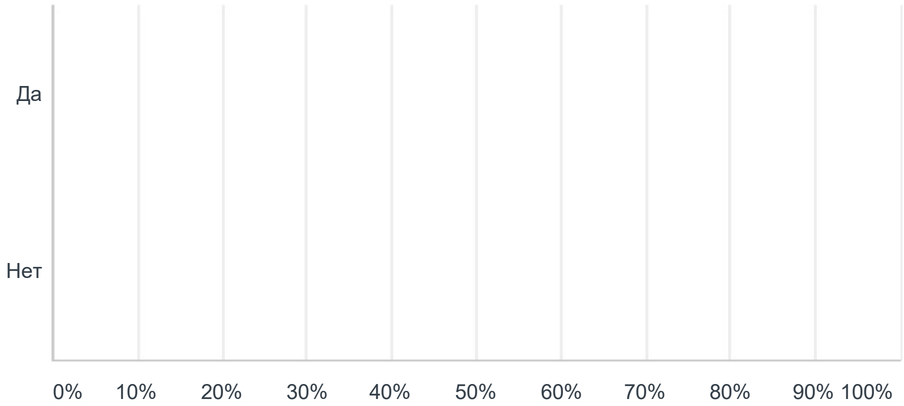


ANSWER CHOICES	RESPONSES	
Да	0.00%	0
Нет	100.00%	1
TOTAL		1

#	ЕСЛИ «ДА» ИЛИ ВЫ ХОТИТЕ ОСТАВИТЬ КОММЕНТАРИЙ, ОПИШИТЕ УЯЗВИМОСТИ ИЛИ ОТСУТСТВИЕ МЕР БЕЗОПАСНОСТИ (ЗАПОЛНИТЕ ПОЛЕ):	DATE
	There are no responses.	

Q10 Считаете ли вы или полагаете, что в процессе управления корневой зоной есть слабые или единичные точки отказа/сбоя (отметьте одно из них)?

Answered: 1 Skipped: 0

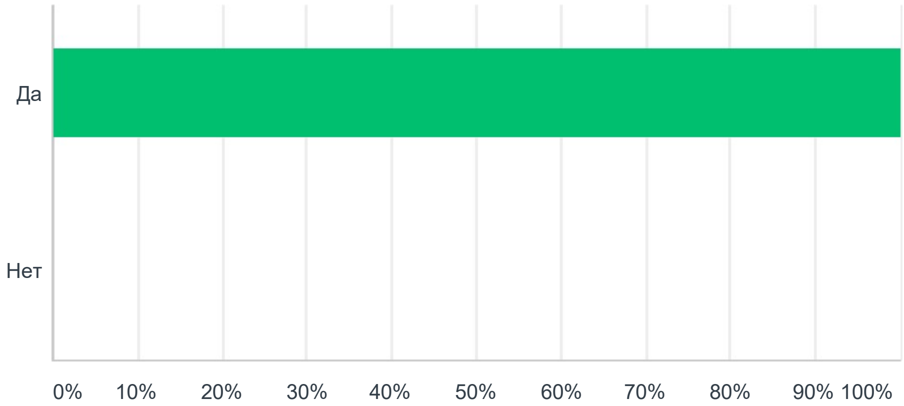


ANSWER CHOICES	RESPONSES	
Да	0.00%	0
Нет	100.00%	1
TOTAL		1

#	ЕСЛИ «ДА» ИЛИ ВЫ ХОТИТЕ СДЕЛАТЬ КОММЕНТАРИЙ, ОПИШИТЕ ЕДИНСТВЕННУЮ ТОЧКУ(И) СБОЯ: (ЗАПОЛНИТЕ ПОЛЕ)	DATE
	There are no responses.	

Q11 Работают ли системы управления и архитектура (инфраструктура) корневой зоны у вас плавно и эффективно (отметьте галочкой один вариант)?

Answered: 1 Skipped: 0

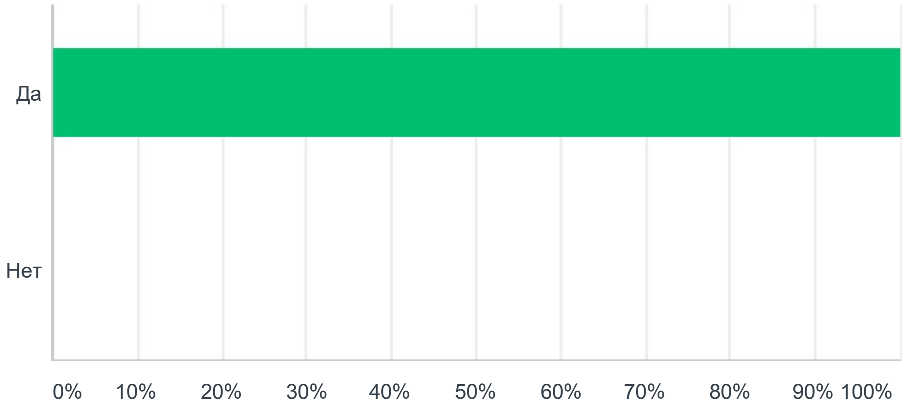


ANSWER CHOICES	RESPONSES	
Да	100.00%	1
Нет	0.00%	0
TOTAL		1

#	ЕСЛИ «НЕТ» ИЛИ ВЫ ХОТИТЕ ОСТАВИТЬ КОММЕНТАРИЙ, ОПИШИТЕ ОБЛАСТИ, В КОТОРЫХ МОЖНО УЛУЧШИТЬ СИСТЕМУ И АРХИТЕКТУРУ (ИНФРАСТРУКТУРУ) (ЗАПОЛНИТЕ ПОЛЕ):	DATE
	There are no responses.	

Q12 Работают ли системы процессов управления корневой зоной, деловые отношения и коммуникации бесперебойно и эффективно (отметьте галочкой один вариант)?

Answered: 1 Skipped: 0

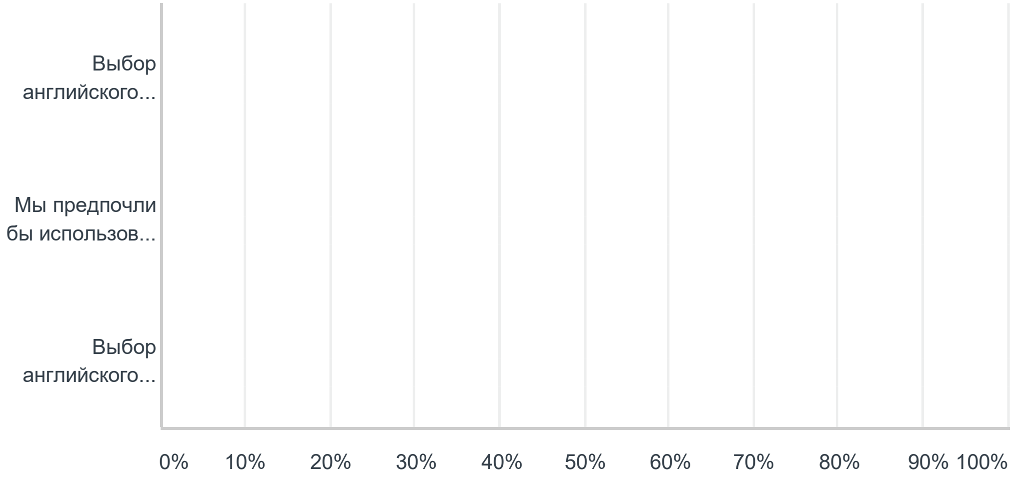


ANSWER CHOICES	RESPONSES	
Да	100.00%	1
Нет	0.00%	0
TOTAL		1

#	ЕСЛИ «НЕТ» ИЛИ ВЫ ХОТИТЕ ОСТАВИТЬ КОММЕНТАРИЙ, ОПИШИТЕ ОБЛАСТИ, В КОТОРЫХ МОЖНО УЛУЧШИТЬ ПЛАВНЫЕ И ЭФФЕКТИВНЫЕ ОПЕРАЦИОННЫЕ СИСТЕМЫ (ЗАПОЛНИТЕ ПОЛЕ):	DATE
	There are no responses.	

Q13 Английский язык является обязательным языком для официальных деловых операций и переписки IANA / PTI. Соответствует ли этот выбор вашим потребностям (отметьте один из вариантов)?

Answered: 1 Skipped: 0

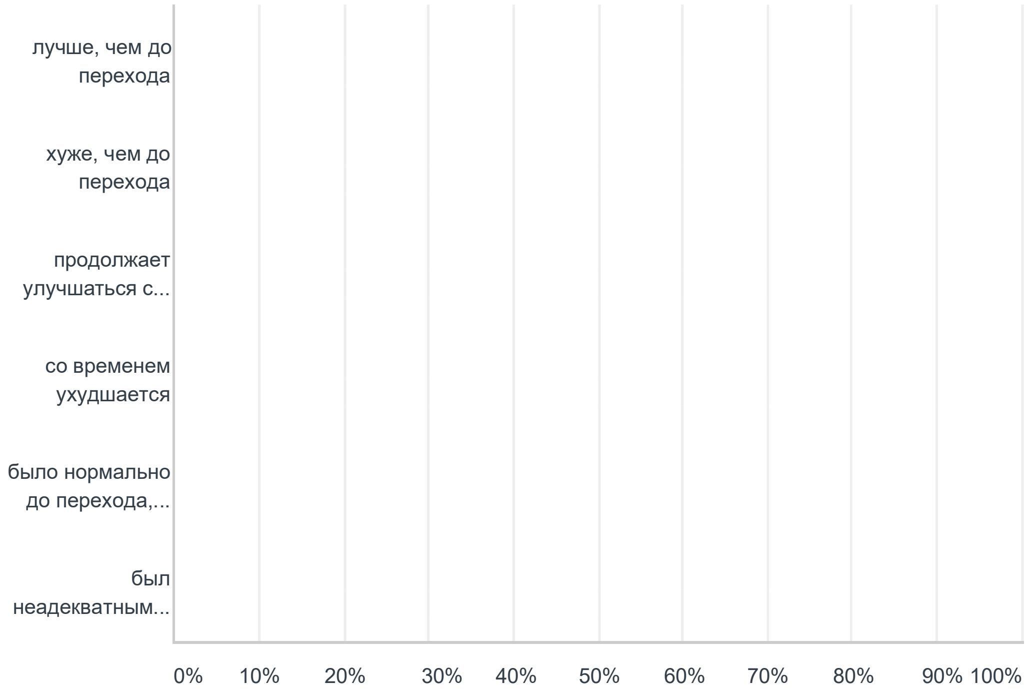


ANSWER CHOICES	RESPONSES	
Выбор английского языка устраивает.	100.00%	1
Мы предпочли бы использовать наш обычно используемый язык, но можем продолжать работать, используя английский.	0.00%	0
Выбор английского языка представляет собой серьезное препятствие для наших текущих отношений с IANA / PTI или сдерживает наши попытки подать заявку на изменения в управлении корневой зоной.	0.00%	0
TOTAL		1

#	ВЫБРАВ ВАРИАНТ «2» ИЛИ «3» ИЛИ ВЫБРАННЫЙ ЯЗЫК (ЗАПОЛНИТЕ ПОЛЕ):	DATE
	There are no responses.	

Q14 IANA (теперь PTI) стала независимой от правительства США в 2016 году. По вашему мнению, с тех пор эффективность процесса управления корневой зоной (выберите один или несколько):

Answered: 1 Skipped: 0



ANSWER CHOICES	RESPONSES	
лучше, чем до перехода	0.00%	0
хуже, чем до перехода	0.00%	0
продолжает улучшаться с течением времени	0.00%	0
со временем ухудшается	0.00%	0
было нормально до перехода, и теперь все в порядке	100.00%	1
был неадекватным до перехода и неадекватным сейчас	0.00%	0
Total Respondents: 1		

#	ПОЖАЛУЙСТА, УТОЧНИТЕ КОММЕНТАРИЕМ ВЫБРАННЫЕ ВЫШЕ ВАРИАНТЫ (ЗАПОЛНИТЕ ПОЛЕ):	DATE
	There are no responses.	

Q15 Пожалуйста, сделайте любые другие комментарии относительно процесса управления корневой зоной IANA / PTI, в том числе:любые аспекты, которые могут быть улучшены за счет оптимизации или повышения безопасности,области, требующие улучшенной документации, пояснений или прозрачностито, что вы считаете наиболее важными из описанных выше моментов, иобласти данного опроса, в которых вы особенно уверены или не уверены в своих ответах. (заполнить бланк):

Answered: 0 Skipped: 1

#	RESPONSES	DATE
	There are no responses.	

Q16 Здесь, по вашему выбору, вы можете указать конкретную контактную информацию на тот случай, если мы будем запрашивать дополнительную информацию. Если вы включите эту информацию, мы будем использовать ее вместо информации, которую мы использовали для связи с вами:

Answered: 1 Skipped: 0

Подробности этого ответа анонимны JAS Global Advisors. / Details of this response have been redacted by JAS Global Advisors for confidentiality purposes.

APPENDIX B: DATA AND DOCUMENT COLLECTION

APPENDIX B: DATA AND DOCUMENT COLLECTION

This Appendix provides a listing of data and documents requested and received by ICJ.

1. Documentation requested and received from IANA

ICJ requested that IANA provide process documents to support the construction of process flows, systems and architecture, to facilitate the identification of potentially incomplete or duplicative process steps and the stability, security and resiliency of systems. This request included:

1. Process overview documentation (e.g., flow charts, process documentation, roles and responsibilities documentation, contractual requirements/letter agreements, functional requirements) that describes the relationship among the involved parties, the roles and responsibilities of each party and the Service Level Agreements of each party. (Received; elaborated during discussion/interviews)

2. Documentation describing process change control procedures. (Received)

3. A description of material process changes in the past three years including relevant change control documentation/artifacts. (Received)

4. A list of COTS/non-custom software (including open source) used to support this process and dependent processes (include major version/build number). (Materially included in SOC2 report; elaborated during discussion/interviews)

5. A list of non-COTS/custom software used to support this process and dependent processes and the parties that authored the software (whether internally developed or developed by a third party under contract). (Materially included in SOC2 report; elaborated during discussion/interviews)

6. For both COTS and non-COTS software, documentation describing how the software is supported for updates, enhancements, and bug fixes both routine and emergency. (Discussed during discussion/interviews)

7. Software requirements documentation describing the functional requirements of non-COTS/custom software developed to support this process and dependent processes. (Discussed during discussion/interviews)

8. Software Development Lifecycle (SDLC) documentation for all custom developed software including design requirements, testing requirements, run/operational requirements, and evidence that the SDLC has been followed for the past three years. (Discussed during discussion/interviews)

9. Security requirements documentation describing the security requirements and assertions of each party, relevant Service Level Agreements related to security including incident reporting requirements and timelines. (Received; elaborated during discussion/interviews)

10. Security policy documents covering this process and dependent processes for all involved organizations including technical and non-technical controls, and review and audit requirements. (Received; elaborated during discussion/interviews)

11. All third-party audits completed in the past three years for systems and processes with scope covering this process or dependent processes. Please include any non-public components of these reports including deficiency/remediation content, POAMs, and similar. (Received)

12. A list of security/control/risk frameworks used by the organizations, how the organization uses the framework, and whether the organization's use of the framework is required by contract or regulatory body. (Received; elaborated during discussion/interviews)

13. A list of critical personnel listing titles, functions, and tenure of continuous employment. Do not provide employee names; please identify personnel only by "Individual 1", "Individual 2", etc., or tokens. (Received; elaborated during discussion/interviews)

14. Relevant security-related Human Resources policies for the aforementioned critical personnel including but not limited to background screening requirements and drug screening requirements. Do not provide results only the policies. (Materially included in SOC2 report; elaborated during discussion/interviews)

15. Business continuity and disaster recovery plans and documentation for this process and dependent processes. (Received)

16. Documentation, including exercise design and After-Action Reporting (AAR), describing exercises of continuity of business, disaster recovery, and security procedures. (Received)

17. Technical requirements for authoritative name servers: the technical tests IANA performs for delegation changes in the root zone including changes to the name server set (NS records) and any associated delegation signer (DS) records. (Received)

18. Examples of gTLD Revocation processes including gTLD Revocation Reports. (Received)

2. Survey data

As more fully described in the report body, a survey consisting of 15 questions was sent at the beginning of April to all the TLD managers and technical contacts in the IANA database. It was disseminated by email by different members of the ICJ consortium. The survey – which used a professional account of Survey Monkey - remained open until the third week of April.

In all, 90 survey respondents provided feedback, representing ca. 700 TLDs (of which 60 were ccTLDs from all the regions).

The survey was conducted in English (85 responses), Spanish (4 responses) and Russian (1 response). All responses were duly anonymized in the comments and qualitative feedback sections.

3. Interviews

Eighteen interviews were conducted by different members of the team between May and June 2021. Most were conducted among TLD operators, listed in the table below, as well as the IANA.

.mx	**Afilias**
PIR	**.ma**
NIC.br	**GoDaddy**
ZDNSm	**EURID**
YuWei Registry	**DENIC**
JPRS	**.co**
.zm	**CentralNIC**
.ug	**.be**
.ht	**IANA**

The aim of the interviews were multiple: in the case of those who had responded to the survey they were trying to achieve a greater understanding of some of the outstanding comments received from them and getting a chance to discuss and explore these issues in greater depth. In some other cases interviews were conducted to TLDs that did not respond to the survey, but which represented an interesting vantage point for IANA as customers. This list group was identified following an analysis of RZ changes of the last two years. In the case of the IANA interview mentioned in this section, it was conducted specifically to address comments and questions that emerged from the consultants from the responses received in the survey. The interviews were held with online video conferencing tools (mostly with the Zoom platform) and they were not recorded but notes were taken from these exchanges. Interviews were conducted in English, Chinese, Spanish and French.

4. Information Received from the Root Zone Maintainer

Printed in full on next page.

VERISIGN

September 01, 2021

Via Email

Dear Jeff Schmidt and the JAS-ICJ Team,

In our capacity as responsible stewards of the internet, we can and should be a key contributor to the response to the community request for an RZM study that aimed to "determine[d] whether or not additional checks/balances/verifications are required post transition."[1] Our detailed responses to the first set of questions we received from the RZM study contractor identified concerns about the sensitive nature of information necessary to provide a comprehensive response, as well as the necessity for the contractor to execute a non-disclosure agreement and to attest to their willingness and ability to protect sensitive and confidential information in accordance with our procurement and information security policies. And, as we conveyed to ICANN, many of the questions received seemed well out of scope from the intent of the IANA Stewardship Transition Coordination Group (ICG).

In response to these concerns, the RZM study contractor provided a revised request for information. While the revised request invited us to provide any confidential information "necessary" to support our responses, the contractor also stated that it had "no need or desire to be the processor of sensitive or company-secret data or information." No controls were put in place that would permit the conveyance of such confidential information in any event. As a result, the information provided in this response is designed to be as helpful and responsive as possible without the inclusion of confidential information.

Verisign has served as the Root Zone Maintainer for decades. The overriding mantra that we instill into the culture for all involved staff members is that the root zone must be *unnaturally perfect*. This means that we have a history of doing more than is strictly necessary to ensure the security and stability of the root zone. Over the past decades, Verisign has continuously improved the human and automated processes, system tools, procedures, and security of our root zone management system.

Manual Root Zone Updates

Initially, Verisign received root zone updates via email in the form of template documents. In this era of manual email template processing by humans, several milestones illustrate Verisign's commitment to the security and stability of the root zone:

- Rigor and formality were added to the manual template process between IANA and Verisign, to include PGP verification and processing of emails.

[1] https://www.icann.org/en/system/files/files/iana-stewardship-transition-proposal-10mar16-en.pdf IANA Stewardship Transition Coordination Group (ICG)

- Verisign added further rigor and formality to the manual internal Root Zone Change Request (RZCR) template process, to include two-person review, management review and management approval for each RZCR template.
- Verisign accumulated a list of specific technical checks to identify and avoid potential problems when making various types of root zone changes. We then began automating this process, to ensure the execution of each check on every occasion.

Root Zone Management System

Around 2005, in conjunction with IANA and the NTIA, Verisign began creating an automated root zone management system to handle root zone changes. This system codified the human workflow that had slowly grown and evolved over the years, centralizing all the technical checks, internal approval gates, external approval gates, and security gates that had been added to the manual system. The automated system included more redundancy than was strictly necessary, with redundant architecture and complete, fully capable and configured redundant systems in alternate data centers. As Verisign and IANA embraced an automated solution for handling root zone changes, the following milestones help illustrate Verisign's commitment to security (confidentiality, integrity, and availability) and stability of the root zone:

- In 2008, having invested millions of dollars, and four years of development time across teams in three countries, and after an approval process and successful period of parallel operations with the 'old' manual system, Verisign began using the new automated system.
- To enable a smooth transition from email templates to API usage, Verisign developed a tool to parse the templates and create RZCRs via the EPP API.
- Verisign initiated policies to regularly review internal accounts with access to the new root zone management system, to verify access requirements with the manager of the account holder
- Verisign created a new version of the root zone management system to allow for DNSSEC signing. Both old and new systems were run simultaneously for months to prove that they both flawlessly created zones with the same zone data. In 2010, Verisign's root zone management system was used to create and publish the first DNSSEC signed root zone.
- In preparation for the transition of NTIA's stewardship of the IANA function, Verisign again redesigned the system, to no longer require NTIA authorization. Again, both old and new systems were run in parallel for months to prove that they produced identical zones. In 2016, Verisign began using the newer root zone management system.
- While nearly all processes and functions are fully automated to avoid human error, Verisign introduced new security functionality in the system that provided for two-person approvals by Verisign staff for individual RZCRs, as well as two-person approvals by Verisign staff for each new root zone published. It also separated privilege between two types of access: access that provides the ability to introduce change, and access that provides the ability to approve change. The system enforces that these two types of access are mutually exclusive; to gain one is to lose the other.
- Verisign enforced restrictions on internal access to the UI, to require two-factor authentication through a secure jump host.

Verisign's root zone management system has received countless updates over the years to address issues from the smallest nit to the most meaningful security changes. This continuous improvement includes updates to re-factor for greater efficiency, updates to add or tune technical checks for RZCRs, updates to modernize security and encryption algorithms as they evolve, and updates to add two-factor authentication, multi-party approval processes, and enforce privilege separation. The root zone management system undergoes periodic and/or expedited patching whenever necessary for underlying OS and software updates and vulnerabilities, regular security scanning, and regular audit reviews. We use both internal and commercial mitigation solutions for protection against DDoS attacks. We also use internal and commercial tools to monitor both Verisign and IANA prefixes to detect any routing system (BGP) anomalies.

Information Security, Governance, and Business Resiliency

Verisign maintains a comprehensive information security program specifically designed for our mission of helping to maintain the security and stability of the Domain Name System (DNS) and the Internet.

The continuous availability of Verisign services requires significant investments in planning, infrastructure, and people. Verisign follows the ‘three lines of defense’ model in the risk management and control of our business resiliency program: functions that own and manage risk, functions that oversee risks, and functions that provide independent assurance.

In our first line of defense, operational leaders own and manage risk by adhering to effective internal controls and executing risk and control processes / procedures on a day-to-day basis that align with our corporate resiliency goals and objectives. We operate multiple datacenters and have deployed systems throughout the world that are monitored 24X7 by our Network Operations Center (NOC).

Business and technology resiliency are built into everything we do, based on the best practices and controls defined for the company by our second line of defense - our Governance, Risk, and Compliance (GRC) function. GRC oversees risks to business resilience, by employing subject matter experts to build and maintain a robust business resilience program - including defining control objectives, performing risk analysis, leading exercises, and conducting compliance assessments. We perform regular testing of our business continuity and disaster recovery plans, to ensure that the team is able to effectively and efficiently respond to events, and that the business resilience and crisis management plans are up to date and working as intended. Exercises include personnel ranging from technicians to senior leadership. Verisign has a defined Crisis Response Team (CRT), with dedicated employees trained in leading and responding to resiliency related events. During a recent third-party review of our business resiliency program, our Crisis Management Program was listed as a business resilience strength when compared to other companies.

Our third line of defense is our Internal Audit (IA) function. It reports to the audit committee of our board of directors and maintains a high level of independence and objectivity while providing assurance of the effectiveness of our overall business resilience program, including a comprehensive assessment how the first two lines of defense achieve our control objectives. As a recent example of the strength of our program, in 2020 Verisign activated the business resilience plans in response to the global pandemic without any interruption in service.

Cybersecurity

Verisign focuses on continuous improvement to its cybersecurity defense posture. Verisign incorporates numerous protection layers in a globally distributed infrastructure, to include zero trust principles, network and data segmentation, intrusion detection and prevention, secure system images, multifactor authentication and multi-party authorization, automated ingestion of threat intelligence from an array of sources, extensive end point detection and response security stacks, and real-time attack simulation and security validation, all reporting back to our 24X7 NOC. Verisign’s continuous monitoring program employs a mix of external and internal assessments including red teaming, physical and cybersecurity program reviews and testing, application security testing, phishing exercises, bug bounty programs, regulatory audits, and security framework assessments. Beyond ensuring compliance with all regulatory and contractual obligations, to include Sarbanes-Oxley (SOX) controls that include data security policies and internal controls reporting as a public company, and SOC for Service Organizations, Verisign also leverages the NIST Cybersecurity Framework (CSF) and Center for Internet Security controls as one of several evolving sources for enhancing security standards and establishing target operational profiles for safeguards and to continuously evolve "what good looks like". Our risk management programs also include opensource software assessments, supply chain and vendor management controls, and procurement related controls.

Verisign has an insider threat program modeled after the Carnegie Mellon University (CMU) Software Engineering Institute (SEI), focusing on how threats evolve over time and incorporating information from functions throughout the company to prevent, detect, and respond to insider threats most effectively. Verisign has dedicated staff and guard force, facilities, tools, and resources providing a daily focus on protecting Verisign services and infrastructure, and a Threat Management Team that is trained on recognizing and responding to insider threats.

Verisign has a robust security awareness program to ensure employees stay informed. The program includes policies and standards, mandatory monthly and annual training courses, security controls and framework self-attestations, monthly exercises, and case analysis of external events. A security ambassador program connects personnel from throughout the company back to the information security team for additional training and communication channels reaching all sections of Verisign.

Unnaturally Perfect

Security, stability, integrity, and availability are part of Verisign's DNA - they are built into everything we do. With root zone maintainer responsibilities, Verisign's processes and policies insist that every character of each new root zone file is accounted for. The root zone must be *unnaturally perfect*, and as a result Verisign operates in a continuous improvement culture surrounding the processes that support the creation, DNSSEC signing, validation, and publication of the root zone. Verisign's investment in staff, architecture, development, and hardened systems and secure procedures make that *unnaturally perfect* culture a reality.

JAS-ICJ question	Verisign response
How does the Maintainer authenticate requests allegedly originating from IANA? Please address routine systematic interactions (Verisign RZMS to IANA RZMS) and non-systematic (possibly emergency) interactions occurring among staff using a full range of communications modalities (mobile phones, email, etc.).	Verisign receives all types of Root Zone Change Requests (RZCRs) from IANA via a dedicated Extensible Provisioning Protocol (EPP) service. Connections are allowed only from a small number of source IP addresses provided by IANA; other source addresses are blocked. Verisign uses commercial products and custom-made solutions to monitor BGP routing information for Verisign and IANA prefixes. Connections are authenticated and encrypted using industry-standard Transport Layer Security (TLS) protocols and certificates. Verisign's EPP service verifies that IANA's TLS connection presents a known certificate. Connections with invalid client certificates are logged and rejected. Following TLS certificate checks, IANA's process uses documented EPP API methods to authenticate at the application level using discreet credentials provided by Verisign through secure means. IANA may initiate out-of-band (non-EPP) communication with Verisign by contacting Verisign's customer service via telephone or PGP-signed email. IANA and Verisign staff have pre-shared PGP keys with each other so that email messages can be verified by their signature. Verisign team members receiving a request via Verisign customer service again perform PGP signature verification. Verisign team members may telephone IANA team members to confirm or clarify an RZCR if necessary.

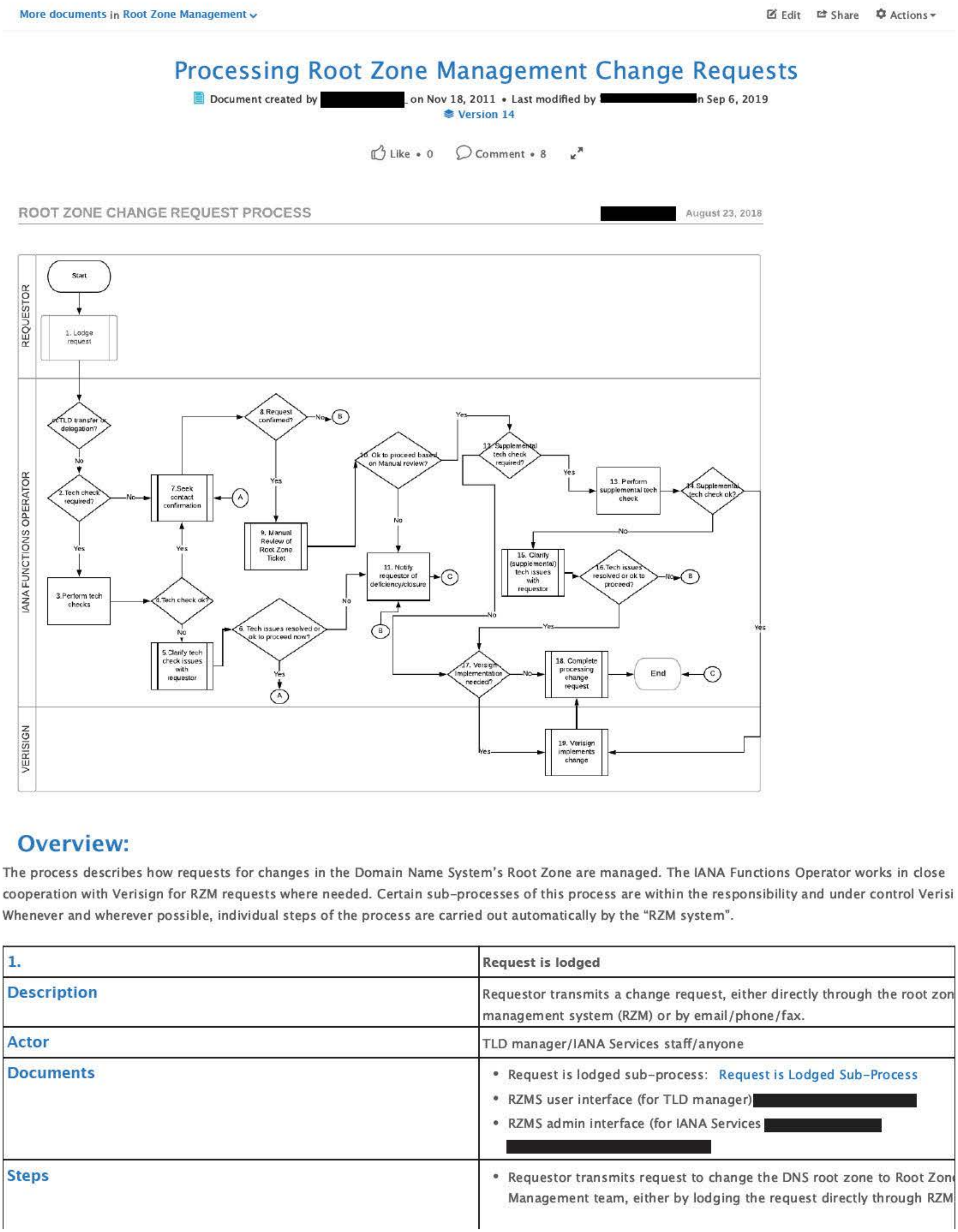
How does the Maintainer ensure that properly authenticated requests are indeed authorized (i.e., not an "out-of-policy" change)?	Verisign only implements RZCRs from IANA that have been properly authenticated. Verisign does not exercise any independent editorial actions of the root zone and does not check change requests for policy correctness. Verisign does evaluate each RZCR for technical accuracy and impact. On rare occasions an RZCR may enter a temporary hold state while Verisign seeks additional guidance and confirmation from IANA.
How are non-systematic (possibly emergency) interactions occurring among staff auenticated, tracked, and audited?	The premise of "non-systematic" interactions might suggest variance from standard operating procedures that does not exist. Emergency changes are sent via EPP like normal changes. The only difference between Emergency and Normal changes is how quickly the change is executed, and how quickly a verified root zone is published. EPP authentication happens as normal. Verisign evaluation for technical correctness and impact happens as normal. Tracking happens within Verisign's root zone management system as normal, and auditing happens within Verisign's root zone management system as normal. Using the same process for both normal and emergency RZCRs eliminates scenarios where mistakes may be made due to using a procedure or process that is unfamiliar or only used on an exception basis.
Please describe the pre-publication review processes used by the Maintainer to prevent the publication of a root zone that is non-DNSSEC verifiable or otherwise erroneous or incomplete. Please describe the processes that limit the Maintainer's staff from accidentally or maliciously introducing out-of-policy changes to the root zone.	Verification for each new candidate zone includes steps like:: 1) Check for a properly formatted zone 2) Check for data accuracy 3) DNSSEC cryptographic verifications 4) Check for expected content 5) Check for unexpected content 6) Manual review and approval to publish by at least two Verisign staff members. Verisign staff are unable to introduce unauthorized changes by virtue of privilege separation and dual approval requirements. The system can allow staff members to manually introduce change requests on behalf of IANA if absolutely necessary, and if staff members are granted access to use the methods of submission. It has been over 4 years since Verisign has received such a request from IANA that would follow this process. The following controls are in place to prevent accidental or malicious change requests: 1) The systems where manual changes can be submitted on IANA's behalf are by default turned off and must be enabled by Verisign's NOC. 2) Staff members do not have permission to make changes until they are temporarily granted such permission by Verisign customer service. 3) Automatic privilege separation ensures that staff members that are given permission to submit changes on IANA's behalf do not simultaneously have permission to approve changes. 4) Every root zone change request, including those received from IANA via EPP, are manually verified and approved by two staff members.
Potential for accidental or malicious errors in the communications path from IANA to the Root Zone Maintainer. JAS-ICJ is aware of two communication paths from IANA to the Maintainer: (i) the programmatic communications occurring between the IANA RZMS and the Maintainer Systems; and (ii) human-to- human (ad hoc and planned) communication among Maintainer and IANA staffs. While programmatic communication is the norm, human to human communication occurs frequently and necessarily during non-standard or emergency changes, when the RZM's supplemental technical checks fail, and in other cases. How does the RZM "close the loop" to ensure that any root zone changes it publishes are authorized and properly implemented and distributed?	With normal and emergency Root Zone Changes, human to human communication is purely supplemental to programmatic EPP RZCR submission. As described above, candidate root zones are extensively verified. Before publication of a new candidate root zone, Verisign maps differences between the previously published root zone and the candidate root zone to approved IANA RZCR in the system. Not detailed above: As each IANA change request is implemented, the database is updated to reflect the change, and the database is again verified against the change to ensure a match is found. Later after a zone is produced from the database, part of verification involves testing the new candidate zone for the presence of the new data represented in the change request. Each individual IANA RZCR is only marked complete after the candidate root zone containing the change is published, and the change has been confirmed through queries to production root name servers. The (i) programmatic case is already described above (e.g. candidate root zone mapped to approved changes). For (ii) there are two sub cases. Either Verisign receives PGP-signed and verified emails, or the out-of-band communication only serves to approve or reject an RZCR already in the system. There is never a case where a change is made that isn't cryptographically tied back to IANA.
JAS-ICJ is aware of the supplemental technical checks performed by the Maintainer prior to publishing root zone changes. To what extent are the Maintainer's "tech checks" the same as IANA's (in purpose and execution) and to what extent do they differ?	Verisign has not performed a review of IANA technical checks. Verisign and IANA may execute some technical checks in common. The methods of performing each check certainly differ by code base and technical implementation, and the weight assigned to each check may differ.

We also understand that given the relatively low volume of root zone change requests, some level of manual review by experts occurs to protect the root zone from any set of situations that “just don’t look right.” Please describe the Maintainer’s approach to manual expert human review.	Every RZCR is reviewed by two Verisign staff members. The purpose of this is to verify that the automated technical checks did not result in any warnings or errors. If any warnings or errors are found, the RZCR is placed on hold until corrected or verified by IANA. Certain significant changes, such as the removal or addition of a TLD, or changes to all of a TLD’s name servers or DS records are always flagged for additional scrutiny. Every candidate root zone is reviewed by at least two Verisign staff member(s). The purpose of this is to verify that the automated technical checks (described previously) did not result in any errors or warnings. If any warnings or errors are found, publication of the zone is postponed until they are resolved.
Potential for accidental outages or malicious actions related to the telecommunications infrastructure serving IANA and the Root Zone Maintainer. Such outages or actions could be related to the infrastructure shared with ICANN. JAS-ICJ has reviewed the business continuity and disaster recovery materials provided by IANA. Please describe any infrastructure that is known to be shared with IANA and the business continuity plans to address a lack of availability of said infrastructure for any reason.	None.
Please describe other relevant business continuity plans designed to restore communication between the Maintainer and IANA should standard communications paths become unavailable.	BCP plans have been provided to ICANN. Verisign’s “normal” business includes a high degree of redundancy at all layers as well as redundant standby options to help maintain availability through the loss of one or many components required for the service.

Sincerely,

Patrick S. Kane
Senior Vice President
VeriSign, Inc.

APPENDIX C: RZM PROCESS AND SUB-PROCESSES (REDACTED)



More documents in Root Zone Management
Edit
Share
Actions

Processing Root Zone Management Change Requests

Document created by [redacted] on Nov 18, 2011 • Last modified by [redacted]n Sep 6, 2019
Version 14

ROOT ZONE CHANGE REQUEST PROCESS [redacted] August 23, 2018

REQUESTOR
IANA FUNCTIONS OPERATOR
VERISIGN
Start
1. Lodge request
0.ccTLD transfer or delegation?
No
2.Tech check required?
No
Yes
3.Perform tech checks
4.Tech check ok?
Yes
No
5.Clarify tech check issues with requestor
6. Tech issues resolved or ok to proceed now?
Yes
A
No
7.Seek contact confirmation
A
8.Request confirmed?
No
B
Yes
9. Manual Review of Root Zone Ticket
10. Ok to proceed based on Manual review?
No
Yes
11. Notify requestor of deficiency/closure
C
B
12. Supplemental tech check required?
Yes
No
13. Perform supplemental tech check
14.Supplemental tech check ok?
No
Yes
15. Clarify (supplemental) tech issues with requestor
16.Tech issues resolved or ok to proceed?
No
B
Yes
17. Verisign Implementation needed?
No
Yes
18. Complete processing change request
End
C
19. Verisign implements change

Overview:

The process describes how requests for changes in the Domain Name System's Root Zone are managed. The IANA Functions Operator works in close cooperation with Verisign for RZM requests where needed. Certain sub-processes of this process are within the responsibility and under control Verisi
Whenever and wherever possible, individual steps of the process are carried out automatically by the "RZM system".

1.	**Request is lodged**
Description	Requestor transmits a change request, either directly through the root zon management system (RZM) or by email/phone/fax.
Actor	TLD manager/IANA Services staff/anyone
Documents	• Request is lodged sub-process: Request is Lodged Sub-Process • RZMS user interface (for TLD manager) [redacted] • RZMS admin interface (for IANA Services [redacted]
Steps	• Requestor transmits request to change the DNS root zone to Root Zon Management team, either by lodging the request directly through RZM

	or by submitting a change request template via email tc root-mgmt@icann.org or by other means (phone/fax/mail). • If a request is not lodged directly through RZMS, IANA Services staff lodges the request on behalf of the TLD manager through RZMS. • A reference number for the request is automatically generated and supplied to the requestor. • Proceed to **Step 2.**

2.	**Tech check required?**
Description	Decision, in which it is determined, whether the requested changes require technical checks.
Actor	RZMS
Documents	N/A
Steps	• System automatically determines whether the change request type requires technical checks. • Yes, if the request includes modifications to name servers and/or ds records, then proceed to **Step 3.** • No, if the request does not include modifications to name servers or d records, then go to **Step 7.**

3.	**Perform technical checks**
Description	Action, in which the supplied root zone change data are checked for compliance with technical requirements.
Actor	RZMS
Documents	RZMS automatically runs each check defined in: • Name server requirements: http://www.iana.org/procedures/nameserver-requirements.htm • DS records requirements: http://www.iana.org/procedures/root-dnssec-records.html • RZM automatically performs the following technical checks:
Steps	– MinimumNameServersAndNoReservedIPsCheck – MinimumNetworkDiversityCheck – NameServerCoherencyCheck – SerialNumberCoherencyCheck – MaximumPayloadSizeCheck – DSCheck – RRSigCheck • Proceed to **Step 4.**

4.	**Tech check ok?**
Description	Decision to determine whether the request passes the technical check step
Actor	RZMS
Documents	• Name server requirements: http://www.iana.org/procedures/nameserver-requirements.htm • DS records requirements: http://www.iana.org/procedures/root-dnssec-records.html
Steps	• RZMS will automatically move request forward if there are no technical errors identified. • Yes, if it passes the tech check, go to **Step 7.** • No, if it doesn't pass the tech check, proceed to **Step 5.**

5.	**Clarify tech check issues with requestor**
Description	Sub-process, in which RZMS, and sometimes IANA Services staff, communicates with the requestor about technical issues which were identified during the tech check.
Actor	RZMS/IANA Services staff
Documents	• Clarify tech check issues with requestor sub-process Clarify Tech Issues with Requestor Sub-Process
Steps	• Interaction between the RZMS system and the requestor to remedy the technical issues identified during the previous steps. If the requestor has questions or a more detailed explanation is required, IANA Service staff interacts with requestor to clarify technical issues. • Proceed to **Step 6.**

6.	**Tech issues resolved or ok to proceed now?**
Description	Decision to determine whether the technical issues have been resolved
Actor	RZMS or IANA Services staff
Documents	N/A
Steps	• If subsequent tests show that the technical errors have been remedied RZMS will automatically move request to the next step. • If the identified errors can be bypassed after the TLD manager has provided a sufficient explanation as to why the request should be processed despite technical errors, IANA Services staff may choose to manually move the request to the next state (AC/TC). • Yes, if the technical errors have been remedied or a sufficient explanation has been provided, then go to **Step 7.** • No, if technical errors have not been remedied and no explanation has been provided by TLD managers, then proceed to **Step 11.**

7.	**Seek contact confirmations**
Description	Sub-process to obtain confirmations from contacts to implement changes.
Actor	RZMS/IANA Services staff
Documents	• Seek contact confirmations sub-process: [redacted]
Steps	• RZM automatically performs the contact confirmation sub-process as described in [redacted] • Proceed to **Step 8.**

8.	**Request confirmed?**
Description	Decision to determine whether all the relevant contacts agree to the change.
Actor	RZMS or IANA Services staff
Documents	N/A
Steps	• System automatically determines whether TLD contacts agree to the change.

	• If the confirmations are provided in such a way that the RZMS system cannot automatically evaluate the reply, IANA Services staff determines whether the proper confirmations have been received. • Yes, if all relevant contacts could be reached and did approve the intended change, then, proceed to**Step 9.** • No, if not all relevant contacts could be reached and/or some of the contacts did not approve the intended change, then, go to **Step 11.**

9.	**Analyze and prepare requested changes**
Description	Sub-process, in which the requested changes are analyzed and prepared.
Actor	IANA Services staff
Documents	Manual Review of Requested Changes Subprocess
Steps	• Perform the sub-process to analyze and prepare the requested changes as described in Manual Review of Requested Changes Subprocess • Proceed to **Step 10.**

10.	**Is it OK to proceed based on Manual Review?**
Description	Decision is the outcome of whether the analysis and preparation could be performed successfully.
Actor	IANA Services staff
Documents	Manual Review of Requested Changes Subprocess
Steps	• Yes, if the analysis and preparation were successful, then go to **Step 11.** • No, if analysis and preparation were not successful, then proceed to **Step 12.**

11.	**Notify requestor of deficiency/closure of their request**
Description	Inform requestor that the changes cannot be implemented due to deficiency.
Actor	RZMS or IANA Services staff
Documents	N/A
Steps	• **In case of deficiency:** Inform the requestor that their request was deficient, stating the reason for deficiency. Wait X Days setting the ticket to Y state until information is received. • **In case of rejection/lack of clarification from the requestor:** Mark the ticket as rejected or admin-close and resolve the ticket. A ticket is rejected by a TLD contact. A ticket is admin-closed by IFO due to a deficiency. • Go to END

12.	**Supplemental tech check required?**
Description	Decision, in which it is determined, whether supplemental tech check is required.
Actor	RZMS
Documents	N/A
Steps	• System automatically determines whether the change request type requires supplemental technical checks. • Yes, if additional tech check is required, then proceed to**Step 13.**

	• No, if no additional tech check is required, then go to **Step 17.**

13.	**Perform supplemental tech check**
Description	Action, to check the supplied root zone change data for compliance with IANA's technical requirements.
Actor	RZMS
Documents	• Name server requirements: http://www.iana.org/procedures/nameserver-requirements.htm • DS records requirements:http://www.iana.org/procedures/root-dnssec-records.html • RZM automatically performs the following technical checks:
Steps	– MinimumNameServersAndNoReservedIPsCheck – MinimumNetworkDiversityCheck – NameServerCoherencyCheck – SerialNumberCoherencyCheck – MaximumPayloadSizeCheck – DSCheck – RRSigCheck • Proceed to **Step 14.**

14.	**Supplemental tech check ok?**
Description	Determine whether the request passes the supplemental technical check step.
Actor	RZMS
Documents	• Name server requirements: http://www.iana.org/procedures/nameserver-requirements.htm • DS records requirements:http://www.iana.org/procedures/root-dnssec-records.html
Steps	• RZMS will automatically move request forward if there are no technical errors identified. • Yes, if it passes the tech check, go to**Step 19 .** • No, if it doesn't pass the tech check, proceed to **Step 15.**

15.	**Clarify supplemental tech issues with requestor**
Description	Sub-process, in which RZM, and sometimes IANA Services staff, communicates with the requestor about technical issues which were identified during the tech check.
Actor	RZMS or IANA Services staff
Documents	• Clarify Supplemental Tech Issues with Requestor Sub-Process
Steps	• Interaction between the RZM system and the requestor to remedy the technical issues identified during the previous steps. If the requestor has questions or a more detailed explanation is required, IANA Service staff interacts with requestor to clarify technical issues. • Proceed to **Step 16.**

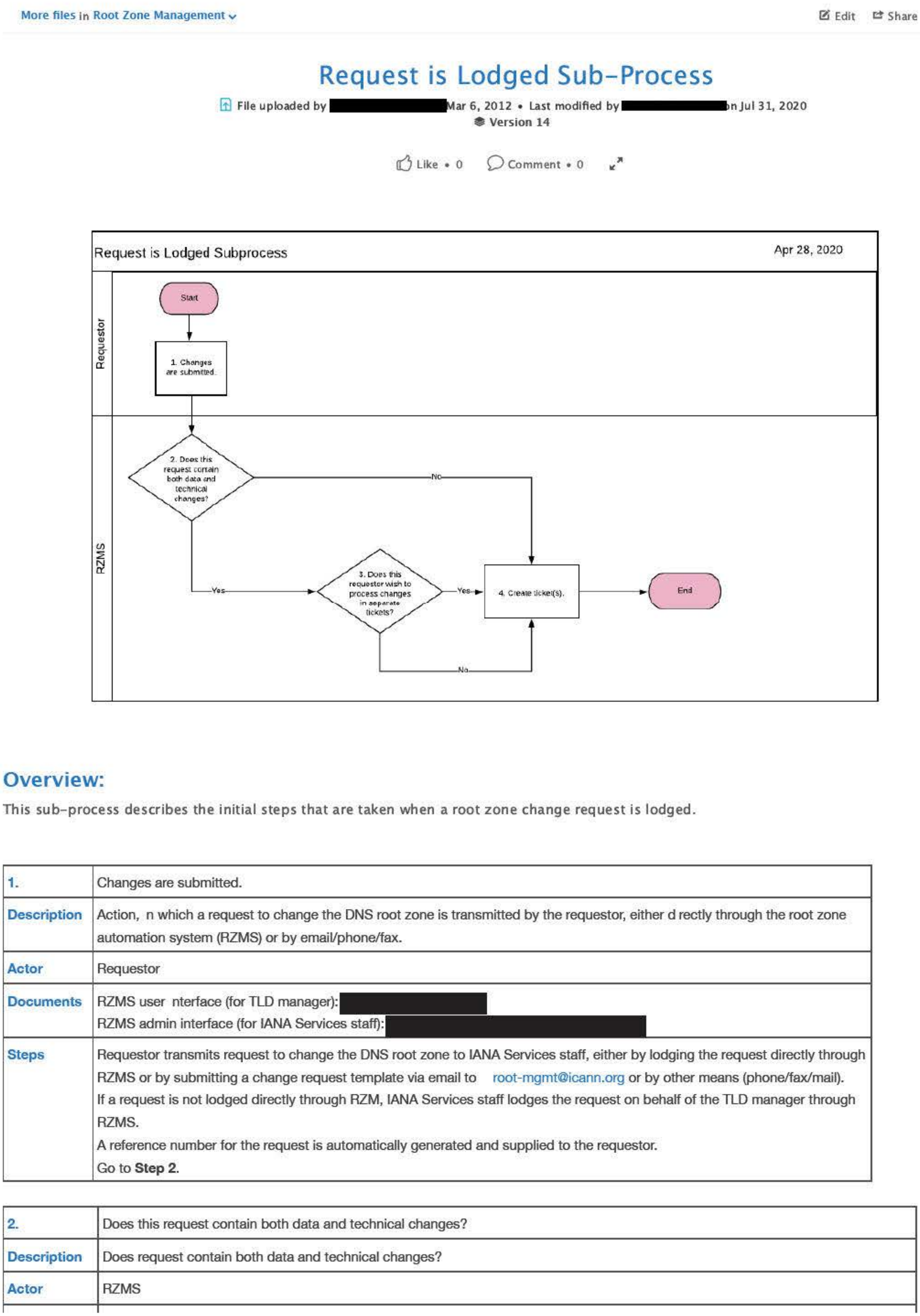
16.	**Tech issues resolved or ok to proceed?**
Description	Decision, in which it is determined, whether the technical issues have been resolved.
Actor	RZMS or IANA Services staff

Documents	N/A
Steps	• If subsequent tests show that the technical errors have been remedied. RZM will automatically move request to the next step. • If the identified errors can be bypassed after the TLD manager has provided a sufficient explanation as to why the request should be processed despite technical errors, IANA Services staff may manually move the request to the next state. • Yes, if the technical errors have been remedied or a sufficient explanation has been provided, then proceed to **Step 17.** • No, if technical errors have not been remedied and no explanation has been provided by TLD managers, then go to **Step 11.**

17.	**Verisign implementation needed?**
Description	Determine whether the change involves changing the root zone file.
Actor	RZMS
Documents	N/A
Steps	• Yes, if the change involves a root zone change (i.e. NS or DS records), go to **Step 19** • No, if the change does not involve a root zone change, go to **Step 18**

18.	**Complete processing of the request**
Description	Sub-process, in which processing of the request is completed. This sub-process has different variations, depending on whether Verisign implementation has to be executed.
Actor	RZMS
Documents	• see Complete Processing of the Request Sub-Process
Steps	• The system performs the complete processing of the request sub-process as described in Complete Processing of the Request Sub-Process. • END

19.	**Verisign implements requested changes**
Description	Verisign implements the authorized change into the root zone itself
Actor	Verisign
Documents	N/A
Steps	• This sub-process is within the responsibility of Verisign. Once complete: • Go back to **Step 18**



More files in Root Zone Management
Edit
Share
Actions
Like • 0
Comment • 0

Request is Lodged Sub-Process

File uploaded by [redacted] Mar 6, 2012 • Last modified by [redacted] on Jul 31, 2020
Version 14

Request is Lodged Subprocess
Apr 28, 2020
Requestor
RZMS
Start
1. Changes are submitted.
2. Does this request contain both data and technical changes?
No
Yes
3. Does this requestor wish to process changes in separate tickets?
Yes
No
4. Create ticket(s).
End

Overview:

This sub-process describes the initial steps that are taken when a root zone change request is lodged.

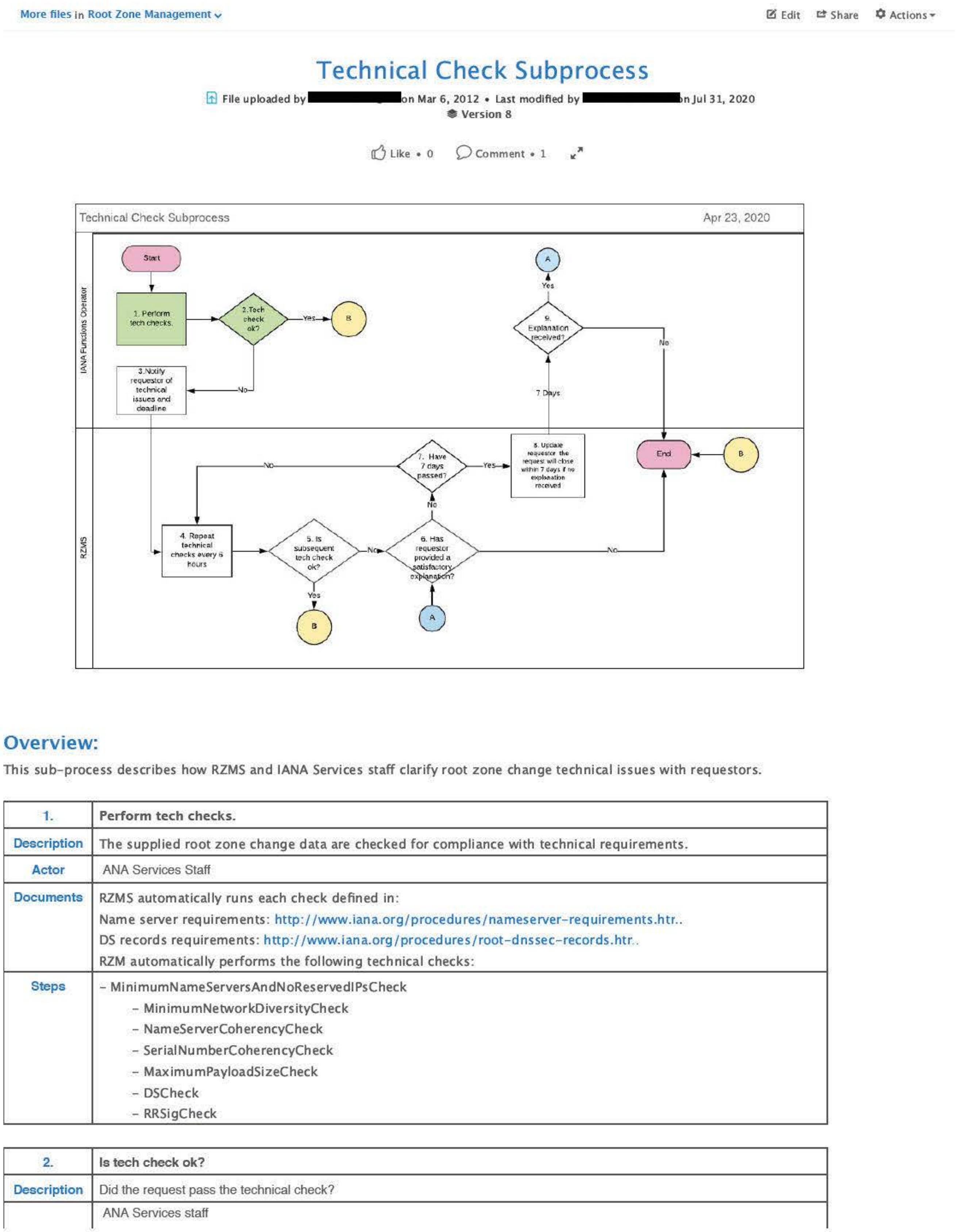
1.	Changes are submitted.
Description	Action, n which a request to change the DNS root zone is transmitted by the requestor, either d rectly through the root zone automation system (RZMS) or by email/phone/fax.
Actor	Requestor
Documents	RZMS user nterface (for TLD manager): [redacted] RZMS admin interface (for IANA Services staff): [redacted]
Steps	Requestor transmits request to change the DNS root zone to IANA Services staff, either by lodging the request directly through RZMS or by submitting a change request template via email to root-mgmt@icann.org or by other means (phone/fax/mail). If a request is not lodged directly through RZM, IANA Services staff lodges the request on behalf of the TLD manager through RZMS. A reference number for the request is automatically generated and supplied to the requestor. Go to **Step 2**.

2.	Does this request contain both data and technical changes?
Description	Does request contain both data and technical changes?
Actor	RZMS

Documents	RZMS admin interface: [redacted]
Steps	RZMS automatically determines whether the request ncludes both data and technical changes. If yes, go to **Step 3.** If no, go to **Step 4.**

3.	Does this requestor wish to process changes in separate tickets?
Description	Does requestor want to process the data and technical changes in separate tickets?
Actor	RZMS and Requestor
Documents	RZMS user interface (for TLD manager)[redacted] RZMS admin interface (for IANA Services staff)[redacted]
Steps	RZMS offers the requestor the option to split their request into separate tickets. In some cases, splitting the ticket will speed up the processing of the request. The requestor either selects the option to split the ticket or selects the option to process all changes in one request. If yes, create 2 tickets in**Step 4.** If no, create 1 ticket in **Step 4.**

4.	Create separate ticket(s)
Description	RZMS creates new relevant tickets for the request
Actor	RZMS
Documents	RZMS admin interface:[redacted]
Steps	If coming from Step 2: RZMS creates one ticket. If coming from Step 3: RZMS creates one/two ticket(s). **END.**



More files in Root Zone Management
Edit
Share
Actions

Technical Check Subprocess

File uploaded by [redacted] on Mar 6, 2012 • Last modified by [redacted] on Jul 31, 2020
Version 8

Technical Check Subprocess
Apr 23, 2020
IANA Functions Operator
RZMS
Start
1. Perform tech checks.
2.Tech check ok?
Yes
B
No
3.Notify requestor of technical issues and deadline
4. Repeat technical checks every 6 hours
5. Is subsequent tech check ok?
Yes
B
No
6. Has requestor provided a satisfactory explanation?
A
No
7. Have 7 days passed?
No
Yes
8. Update requestor the request will close within 7 days if no explanation received
7 Days
9. Explanation received?
Yes
A
No
No
End
B

Overview:

This sub-process describes how RZMS and IANA Services staff clarify root zone change technical issues with requestors.

1.	Perform tech checks.
Description	The supplied root zone change data are checked for compliance with technical requirements.
Actor	ANA Services Staff
Documents	RZMS automatically runs each check defined in: Name server requirements: http://www.iana.org/procedures/nameserver-requirements.htr.. DS records requirements: http://www.iana.org/procedures/root-dnssec-records.htr.. RZM automatically performs the following technical checks:
Steps	– MinimumNameServersAndNoReservedIPsCheck – MinimumNetworkDiversityCheck – NameServerCoherencyCheck – SerialNumberCoherencyCheck – MaximumPayloadSizeCheck – DSCheck – RRSigCheck

2.	Is tech check ok?
Description	Did the request pass the technical check?
	ANA Services staff

Actor	
Documents	Name server requirements: http://www.iana.org/procedures/nameserver-requirements.htr.. DS records requirements: http://www.iana.org/procedures/root-dnssec-records.htn..
Steps	RZMS will automatically move request forward if there are no technical errors identified. If yes, go to **Step 7.** If no, go to **Step 5.**

3.	**Notify requestor of technical issues and deadline.**
Description	Document in which requestor(s) is notified by email of the technical errors that have been identified A deadline to address the technical issues is set
Actor	ANA Services staff
Documents	Email describing technical errors that have been identified Technical Requirements for Authoritative Name Servers: http://www iana org/procedures/nameserver requirements html DS records requirements: http://www iana org/procedures/root dnssec records html
Steps	ANA Services staff notifies requestor of technical errors possibly identified and sets a deadline for requestor to mend those Proceed to Step 2

4.	**Repeat technical checks (every 6 hours).**
Description	Action in which the RZMS system automatically repeats the technical checks
Actor	RZMS
Documents	RZMS admin interface: [redacted] Technical Requirements for Authoritative Name Servers: http://www iana org/procedures/nameserver requirements html DS records requirements: http://www iana org/procedures/root dnssec records html
Steps	RZMS automatically repeats the technical checks every 6 hours Proceed to Step 3

5.	Subsequent tech check ok ?
Description	Decision to determine whether the subsequent tech check is ok
Actor	RZMS
Documents	RZMS admin interface: [redacted] Technical Requirements for Authoritative Name Servers: http://www iana org/procedures/nameserver requirements html DS records requirements: http://www iana org/procedures/root dnssec records html
Steps	RZMS automatically determines whether the technical issues are ok Yes if the technical issues are ok go to END f technical issues are ok this will deliver a positive result to #6 of the RZMS top level process No if technical errors have been identified proceed to Step 4

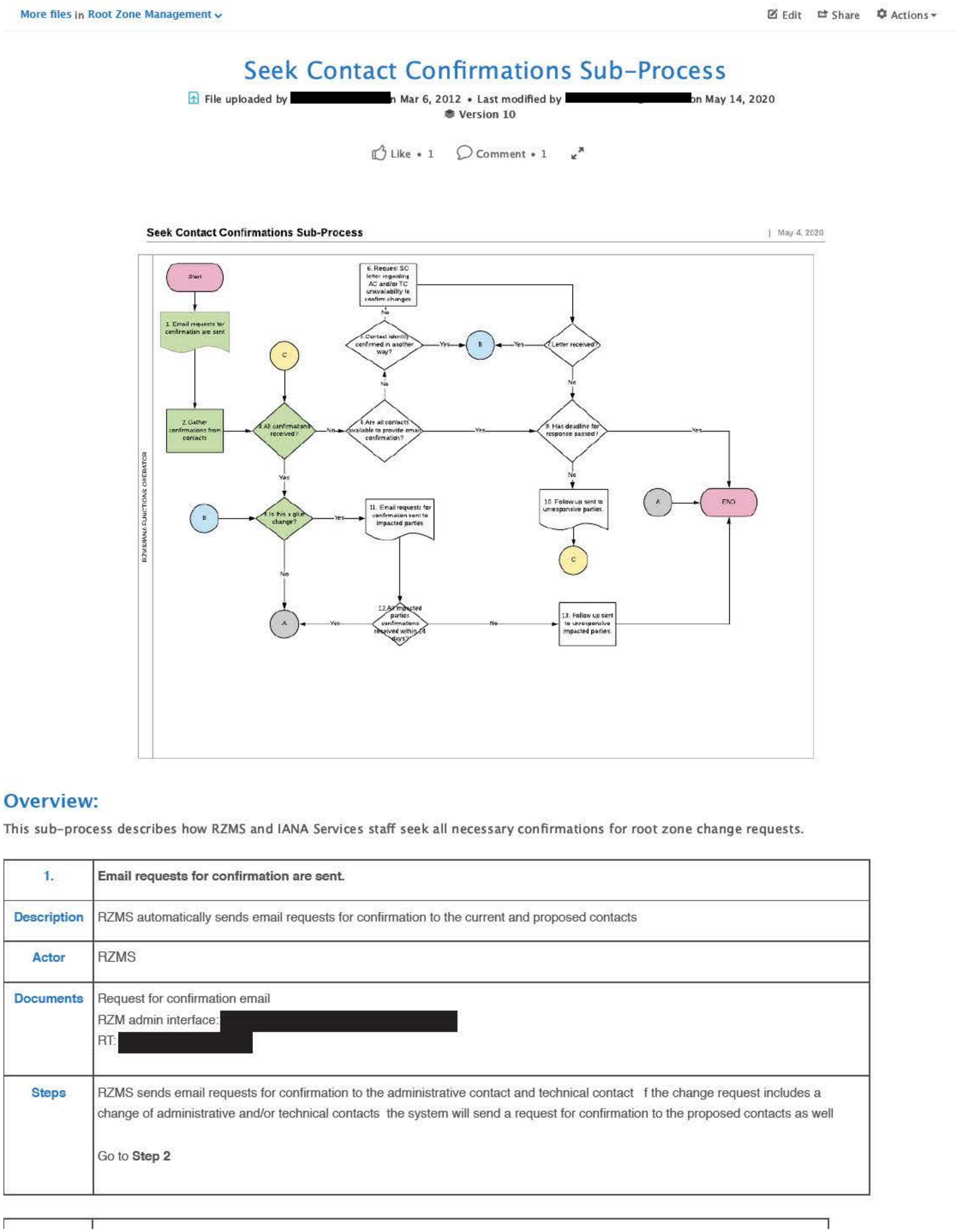
6.	Has requestor provided a satisfactory explanation to proceed to the next step?
Description	Decision in which the RZM system and/or ANA Services staff determine whether an explanation has been provided by the requestor that justifies why the request should proceed despite the technical errors
Actor	RZMS
Documents	RZMS admin interface: [redacted] RT: [redacted]
Steps	f the requestor provides an explanation that justifies why the request should proceed despite the technical errors ANA Services staff will determine whether the request can be manually moved to the next state: Yes if the requestor provides an explanation and ANA Services staff determine it is ok to proceed to the next step go to END This will deliver a positive result to #6 of the RZM top level process

	No if the requestor does not provide an explanation RZM system automatically goes to Step 5

7.	Have 7 days passed?
Description	Decision in which the RZM system automatically determines whether 7 days have passed since the last technical issue notification was sent to the requestor
Actor	RZMS
Documents	RZM admin interface: [redacted]
Steps	The system runs technical checks every 6 hours f technical errors are still present 7 days after the last technical error notification was sent to the requestor another notification will be sent to the requestor RZM automatically determines if 7 days have passed since last technical error notification was sent to requestors Yes if 7 days have passed since the last technical error notification was sent to the requestors go to Step 6 No if 7 days have not yet passed since the last technical error notification was sent to requestors go to Step 2

8.	Update requestor the request will close within 7 days if no explanation received
Description	ANA Services staff will send a reminder to the requestor that their request will close within 7 days unless they send an explanation as to why tech check failed
Actor	ANA Services staff
Documents	RZM admin interface [redacted]
Steps	Once RZMS determines that 7 days have gone by without requestor explaining the reasons for tech check error courtesy reminder is sent by ANA Services staff Requestor will have 7 days to respond Go to Step 7

9.	Explanation received?
Description	ANA Services staff to check RZMS/RT for confirmation of explanation from the requestor
Actor	ANA Services staff
Documents	RZM admin interface: [redacted]
Steps	ANA Services staff checks if there was an explanation received by the requestor within the 7 days deadline f Yes go to Step 4 f No Go to END



More files in Root Zone Management
Edit
Share
Actions

Seek Contact Confirmations Sub-Process

File uploaded by [redacted] n Mar 6, 2012 • Last modified by [redacted] on May 14, 2020
Version 10

Seek Contact Confirmations Sub-Process | May 4, 2020

RZM/IANA FUNCTIONS OPERATOR
Start
1. Email requests for confirmation are sent
2. Gather confirmations from contacts
C
3 All confirmations received?
No
4 Are all contacts available to provide email confirmation?
No
5 Contact identity confirmed in another way?
No
6. Request SO letter regarding AC and/or TC unavailability to confirm changes
Yes
B
Yes
7 Letter received?
No
Yes
9. Has deadline for response passed?
Yes
No
10. Follow up sent to unresponsive parties.
C
A
END
Yes
B
8 Is this a glue change?
Yes
11. Email requests for confirmation sent to impacted parties
No
A
Yes
12.All impacted parties confirmations received within 14 days?
No
13. Follow up sent to unresponsive impacted parties.

Overview:

This sub-process describes how RZMS and IANA Services staff seek all necessary confirmations for root zone change requests.

1.	**Email requests for confirmation are sent.**
Description	RZMS automatically sends email requests for confirmation to the current and proposed contacts
Actor	RZMS
Documents	Request for confirmation email RZM admin interface: [redacted] RT: [redacted]
Steps	RZMS sends email requests for confirmation to the administrative contact and technical contact f the change request includes a change of administrative and/or technical contacts the system will send a request for confirmation to the proposed contacts as well Go to **Step 2**

2.	**Gather confirmations from contacts.**
Description	RZMS and/or ANA Services staff gather responses to the email requests for confirmation
Actor	RZMS and/or ANA Services staff
Documents	RZMS admin interface (for ANA staff): [redacted] RT: [redacted]
Steps	RZMS and/or ANA Services staff gathers responses from the old and new administrative and technical contacts RZMS automatically keeps track of responses when TLD managers reply to the request for confirmation emails and when TLD managers login and confirm or reject the request directly through RZM f for some reason RZM cannot parse an email reply ANA Services staff will track the response Go to **Step 3**

3.	**All confirmations received?**
Description	Have all of the necessary contact confirmations been received?
Actor	RZMS and/or ANA Services staff
Documents	RZMS admin interface (for ANA Services staff): [redacted] RT: [redacted]
Steps	RZMS and/or ANA Services staff determine whether confirmations from the administrative and technical contacts have been received f the change request includes a change of administrative and/or technical contacts the system and/or ANA Services staff will determine whether confirmations from both the current and proposed administrative and technical contacts have been received as well f yes go to **Step 8** f no go to **Step 4**

4.	**Are all contacts available to provide email confirmation?**
Description	Are both the administrative and technical contacts available to provide confirmation?
Actor	ANA Services staff
Documents	RT: [redacted]
Steps	ANA Services staff communicates with all parties that have not provided confirmations to remind them they will have 14 days to send their confirmations f yes go to **Step 9** f no go to **Step 5.**

5.	**Contact identity confirmed in another way?**
Description	f the contacts are unable to confirm, can their identity be confirmed n an alternative way?
Actor	ANA Services staff
Documents	N/A
Steps	f yes go to **Step 8** f no go to **Step 6**

6.	**Request SO letter regarding AC and/or TC unavailability to confirm changes.**
Description	ANA Services staff requests a letter from the Sponsoring Organization that confirms the changes on company letterhead signed by an official that then explains why the AC/TC is unable to respond
Actor	ANA Services staff
Documents	RT: [redacted]
Steps	 Go to **Step 7**

7.	**Letter received?**
Description	Was SO letter received?
Actor	IANA Services staff
Documents	RT: [redacted]
Steps	If yes, go to **Step 8.** If no, go to **Step 9.**

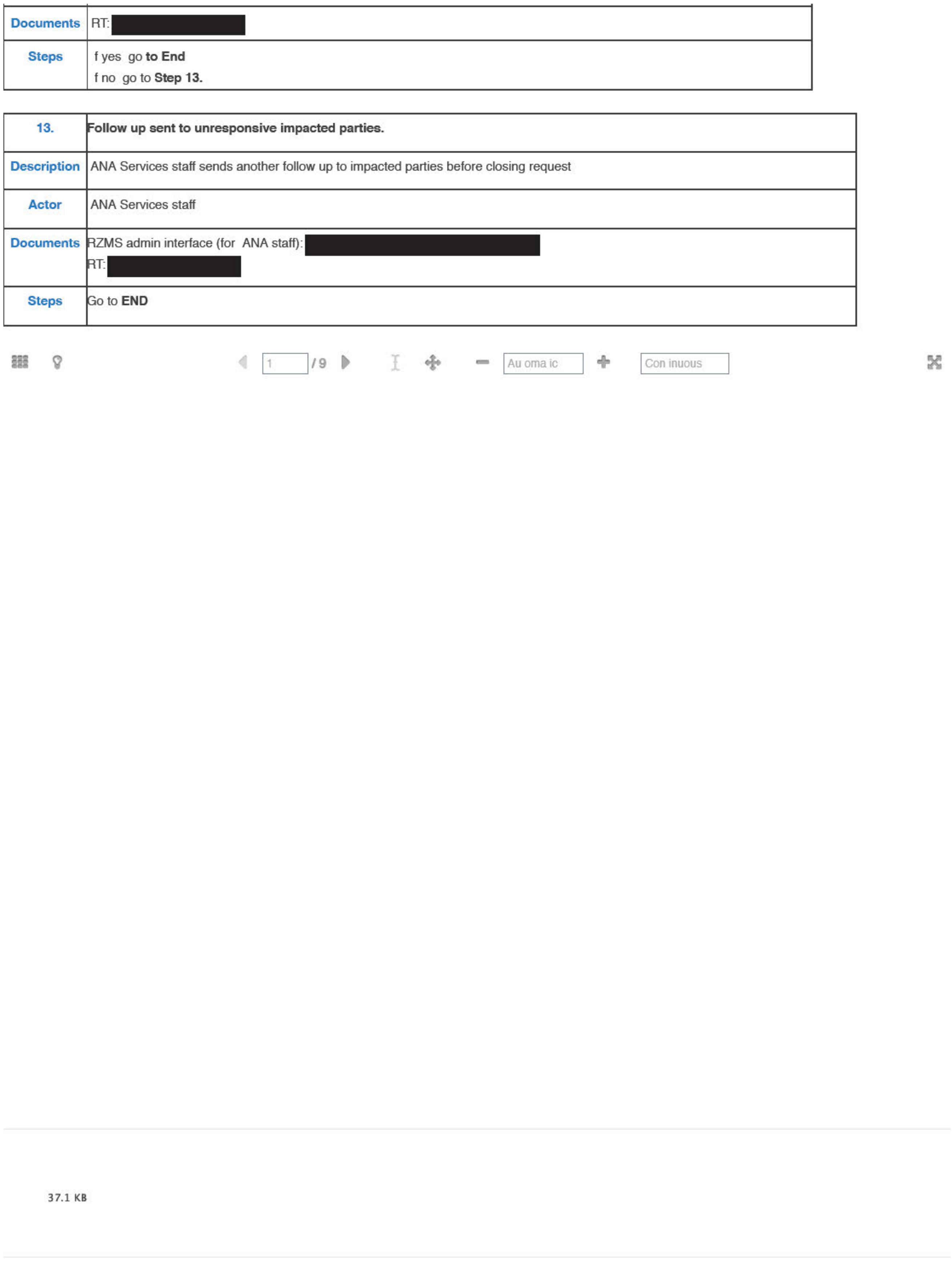
8.	**Is this a glue change?**
Description	s requested change is a glue change?
Actor	RZMS
Documents	RZMS admin interface: [redacted]
Steps	RZM system automatically determines whether the request includes changes to one or more name servers that are shared with any other TLD(s) f yes (request includes a change to one or more shared name servers) go to **Step 11** f no (request does not include changes to a shared name server) go to **END** This will deliver a positive result to #8 of the RZM top level process

9.	**Has deadline for response passed?**
Description	IANA Services staff determ nes whether to close ticket or follow up with the unresponsive parties.
Actor	IANA Services Staff
Documents	RZMS admin interface: [redacted] RT: [redacted]
Steps	If yes, go to **End**. If no, go to **Step 10.**

10.	**Follow up sent to unresponsive parties.**
Description	ANA Services staff sends follow up to unresponsive parties
Actor	ANA Services staff
Documents	RT: [redacted]
Steps	Go back to **Step 3**

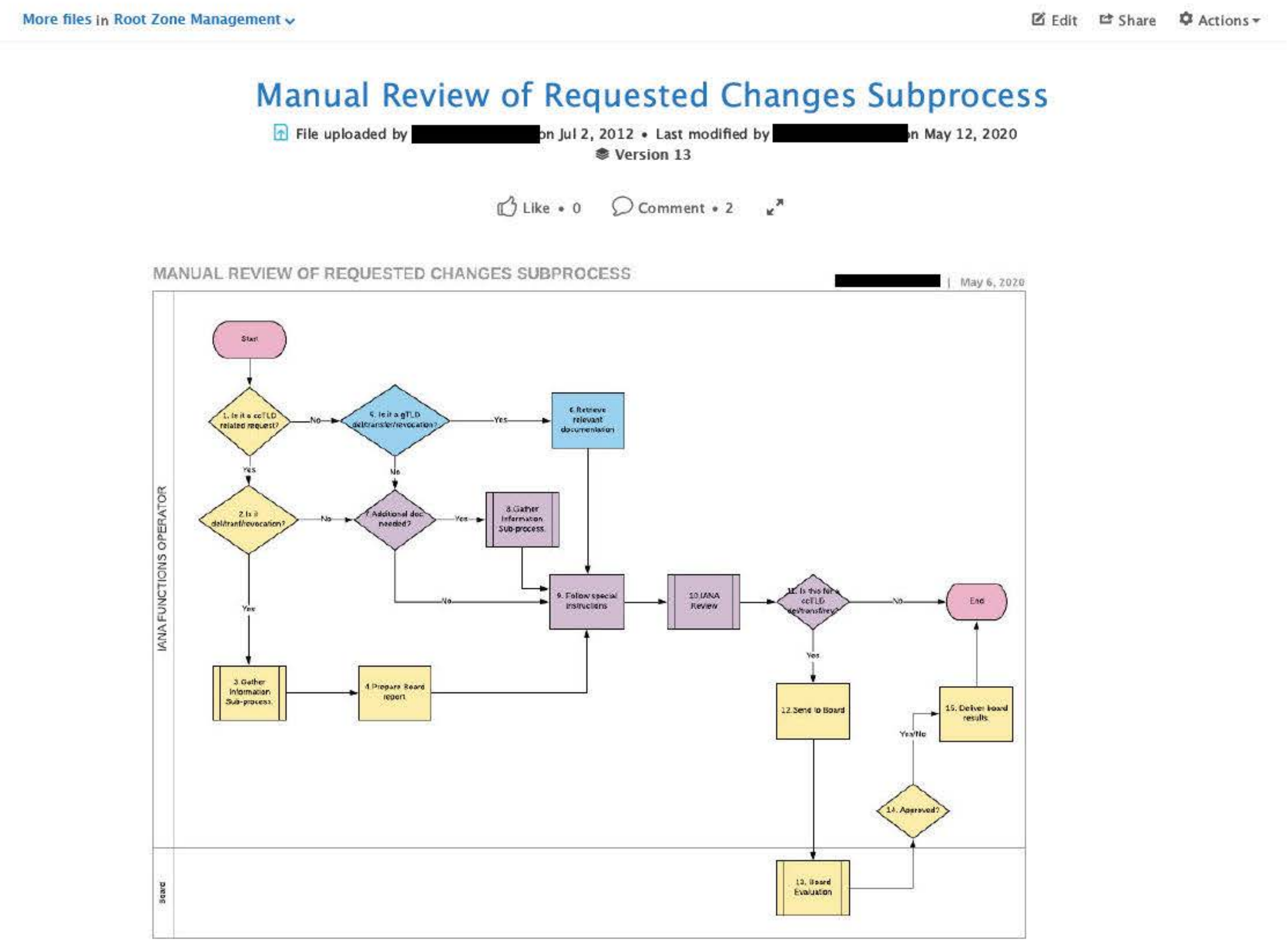
11.	**Email requests for confirmation sent to impacted parties.**
Description	ANA Services staff send confirmation requests to impacted parties
Actor	ANA Services staff
Documents	RZMS admin interface (for ANA staff): [redacted] RT: [redacted]
Steps	ANA Services staff communicates with all parties that have not provided confirmations to remind them they will have 14 days to send their confirmations Go to **Step 12.**

12.	**All impacted parties' confirmations received within 14 days?**
Description	Have all confirmations from impacted parties been received within 14 days?
Actor	ANA Services staff



Documents	RT: [redacted]
Steps	f yes go **to End** f no go to **Step 13.**

13.	**Follow up sent to unresponsive impacted parties.**
Description	ANA Services staff sends another follow up to impacted parties before closing request
Actor	ANA Services staff
Documents	RZMS admin interface (for ANA staff): [redacted] RT: [redacted]
Steps	Go to **END**



More files in Root Zone Management ⌄

Edit Share Actions ▾

Manual Review of Requested Changes Subprocess

File uploaded by [redacted] on Jul 2, 2012 • Last modified by [redacted] on May 12, 2020
Version 13

Like • 0 Comment • 2

MANUAL REVIEW OF REQUESTED CHANGES SUBPROCESS
[redacted] | May 6, 2020
IANA FUNCTIONS OPERATOR
Board
Start
1. Is it a ccTLD related request?
No
5. Is it a gTLD del/transfer/revocation?
Yes
6. Retrieve relevant documentation
Yes
No
2. Is it del/tranf/revocation?
No
7. Additional doc needed?
Yes
8. Gather Information Sub-process.
No
Yes
9. Follow special instructions
10. IANA Review
11. Is this for a ccTLD del/transf/rev?
No
End
Yes
3. Gather Information Sub-process.
4. Prepare Board report
12. Send to Board
15. Deliver board results
Yes/No
14. Approved?
13. Board Evaluation

Overview:

This sub-process describes how IANA Services staff analyzes and prepares requested root zone changes. In this process there will be three possible paths. One for ccTLD and one for gTLDs delegation, transfer or revocations, and one for Routine change requests.

1.	**Is it a ccTLD related request?**
Description	Decision in which ANA Services staff determines if the request is country code related
Actor	IANA Serv ces staff
Documents	RZM admin interface: [redacted] RT: [redacted]
Steps	Review and confirm if the request is ccTLD related f yes go to **Step 2.** f no go to **Step 5.**

2.	**Is it a Delegation, Transfer or Revocation?**
Description	s the request a ccTLD delegation transfer or revocation?
Actor	IANA Serv ces staff
Documents	RZM admin interface: [redacted]

	RT: [redacted]
Steps	Confirm that the request is a ccTLD delegation transfer or revocation f yes go to **Step 3.** f no go to **Step 7.**

3.	**Gather Information Sub-process.**
Description	ANA Services staff emails the requestor the list of documents they need to send
Actor	IANA Serv ces staff
Documents	RZM admin interface: h[redacted] [redacted] RT: [redacted] Gather nformation Sub process
Steps	Email requestor with a list of documents Follow Gather nformation Sub process until all requested documents have been received Go to **Step 4.**

��

4.	**Prepare ICANN Board Report**
Description	IANA Services staff writes the Board report.
Actor	IANA Services staff
Documents	RT: [redacted] Supporting documentation Board report
Steps	Write the PTI Board Report. Go to **Step 9**.

5.	**Is it a gTLD Delegation, Transfer or Revocation?**
Description	s the request a gTLD delegation transfer or revocation?
Actor	IANA Serv ces staff
Documents	RZM admin interface [redacted] RT: [redacted]
Steps	Confirm that the request is a gTLD delegation transfer or revocation f yes go to **Step 6.** f no go to **Step 7.**

6.	**Retrieve relevant documentation.**
Description	ANA Services staff retrieves all relevant information on the request
Actor	IANA Serv ces staff
Documents	Retrieve document from shared drive: [redacted] and Registry Agreements CANN
Steps	Look for all relevant information to complete the request and update the ticket Go to **Step 9.**

7.	**Is additional information needed?**
Description	Is additional information or documentation needed?
Actor	IANA Services staff
Documents	RT: [redacted] Any provided documentation

Steps	Determine whether any additional information is needed. Note: Depending on the type of change request, determine whether any additional information is needed. (for example, admin transfers or ccTLD contact changes) If yes, go to **Step 8.** If no, go to **Step 9.**

8.	**Gather Additional Information Subprocess**
Description	IANA Services staff contacts the requestor to gather additional information.
Actor	IANA Services staff
Documents	RZM admin interface: [redacted] RT: [redacted] [redacted]
Steps	Follow the Gather Additional Information Subprocess Go to **Step 9.**

9.	**Review special instructions**
Description	IANA Services staff review and follow the TLD special instructions, if any.
Actor	IANA Services staff
Documents	RZM admin interface: [redacted]
Steps	Login to RZM and review the domain details. Review special instructions if there are any. Perform outreach if updates are needed. Go to **Step 10**.

10.	**IANA Review**
Description	IANA Services staff follows the IANA review subprocess.
Actor	IANA Services staff
Documents	RZM admin interface: [redacted] RT: [redacted] [redacted]
Steps	Follow IANA Review Subprocess Go to **Step 11.**

11.	**Is it a ccTLD Delegation, Transfer or Revocation?**
Description	Is the request a ccTLD delegation, transfer or revocation?
Actor	IANA Services staff
Documents	RZM admin interface: [redacted] RT: [redacted]
Steps	Confirm that the request is a ccTLD delegation, transfer or revocation. If yes, go to **Step 12.** If no, go to **End.**

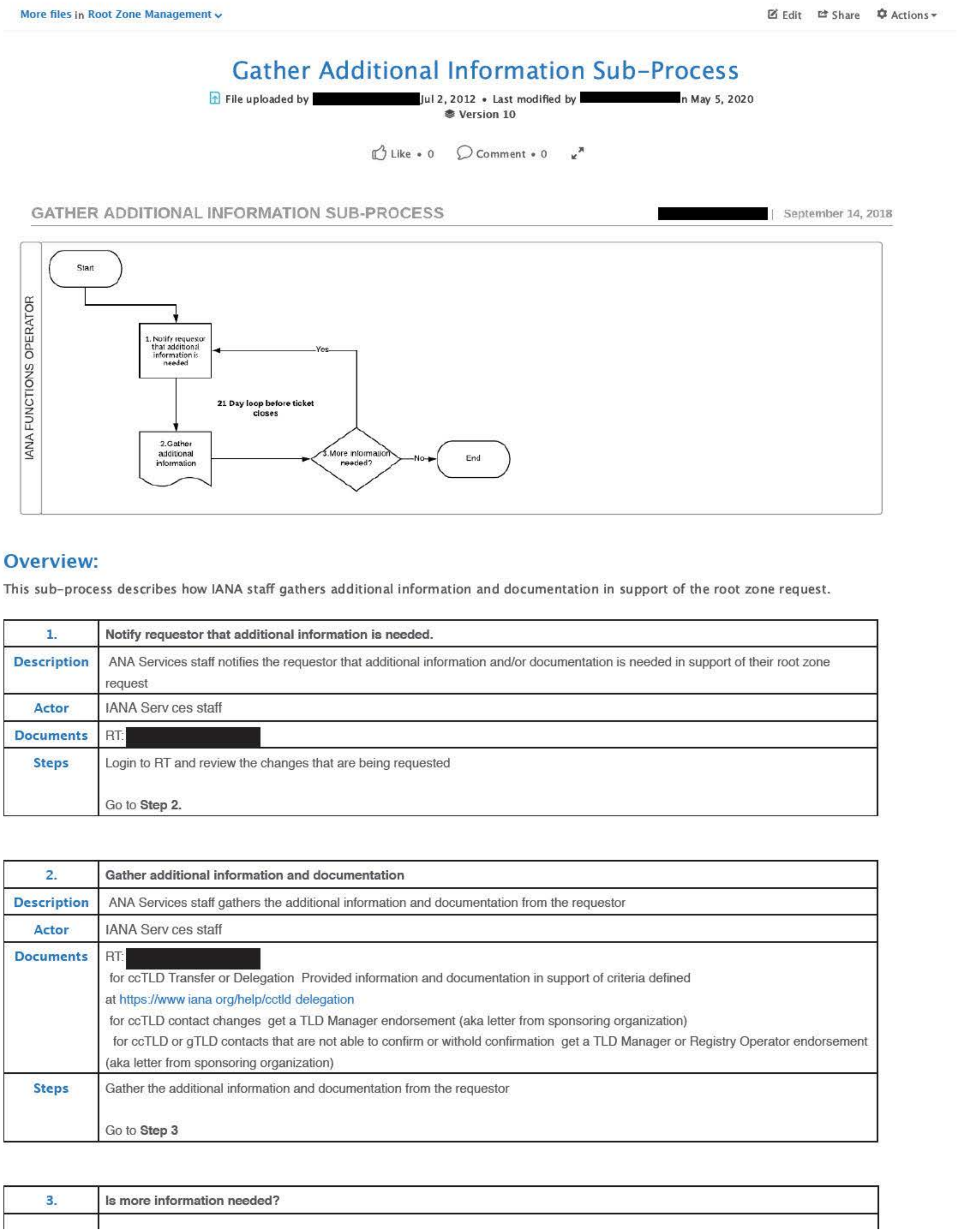
12.	**Submit report to ICANN Board.**
Description	IANA Services staff submits the report to the ICANN Board Secretary.
Actor	IANA Services staff

Documents	ICANN Board report template
Steps	Submit the report to the ICANN Board. Go to **Step 13**.

13.	**Board Evaluation**
Description	The board reviews the report and decides whether or not to approve the request.
Actor	ICANN Board of Directors
Documents	ICANN Board report
Steps	This sub-process is within the responsibility of the ICANN Board of Directors. Go to **Step 14**.

14.	**Approved?**
Description	Did the ICANN Board of Directors approve the request?
Actor	ICANN Board of Directors
Documents	Board meeting minutes. https://www.icann.org/resources/pages/board-of-director_
Steps	Determine whether the ICANN Board of Directors approved the application. Go to **Step 15**.

15.	**Deliver Board results.**
Description	Result is delivered to step #10 of the RZM top-level process.
Actor	IANA Services staff
Documents	RZM admin interface:[redacted] RT:[redacted]
Steps	Deliver a positive result to #10 of the top-level flowchart. Go to **END**.


More files in Root Zone Management
Edit
Share
Actions
Like • 0
Comment • 0

Gather Additional Information Sub-Process

File uploaded by [redacted] Jul 2, 2012 • Last modified by [redacted] n May 5, 2020
Version 10

GATHER ADDITIONAL INFORMATION SUB-PROCESS [redacted] | September 14, 2018

IANA FUNCTIONS OPERATOR
Start
1. Notify requestor that additional information is needed
Yes
21 Day loop before ticket closes
2.Gather additional information
3.More information needed?
No
End

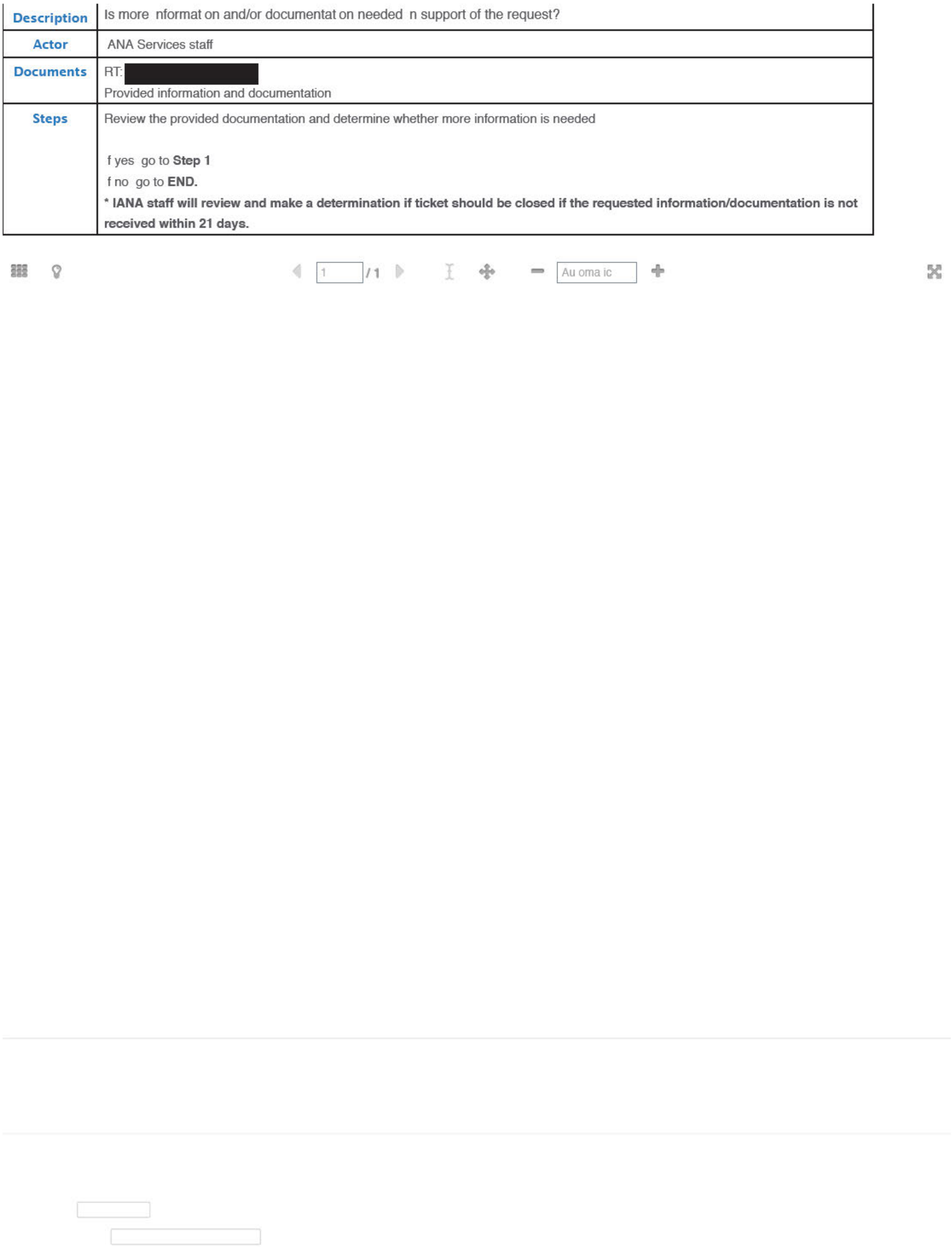
Overview:

This sub-process describes how IANA staff gathers additional information and documentation in support of the root zone request.

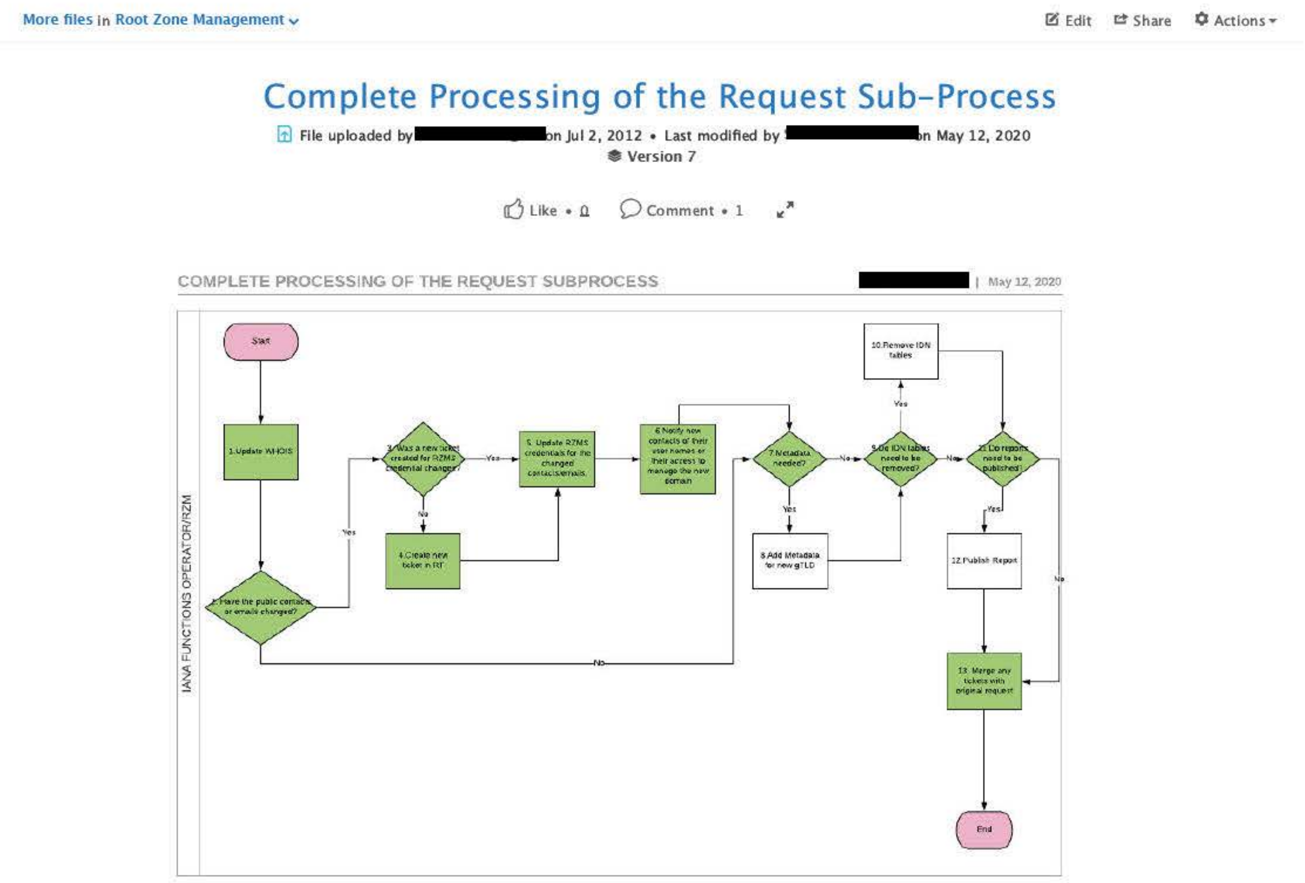
1.	Notify requestor that additional information is needed.
Description	ANA Services staff notifies the requestor that additional information and/or documentation is needed in support of their root zone request
Actor	IANA Serv ces staff
Documents	RT: [redacted]
Steps	Login to RT and review the changes that are being requested Go to **Step 2.**

2.	Gather additional information and documentation
Description	ANA Services staff gathers the additional information and documentation from the requestor
Actor	IANA Serv ces staff
Documents	RT: [redacted] for ccTLD Transfer or Delegation Provided information and documentation in support of criteria defined at https://www iana org/help/cctld delegation for ccTLD contact changes get a TLD Manager endorsement (aka letter from sponsoring organization) for ccTLD or gTLD contacts that are not able to confirm or withold confirmation get a TLD Manager or Registry Operator endorsement (aka letter from sponsoring organization)
Steps	Gather the additional information and documentation from the requestor Go to **Step 3**

3.	Is more information needed?



Description	Is more nformat on and/or documentat on needed n support of the request?
Actor	ANA Services staff
Documents	RT: [redacted] Provided information and documentation
Steps	Review the provided documentation and determine whether more information is needed f yes go to **Step 1** f no go to **END.** *** IANA staff will review and make a determination if ticket should be closed if the requested information/documentation is not received within 21 days.**



More files in Root Zone Management ⌄
Edit
Share
Actions ▾

Complete Processing of the Request Sub-Process

File uploaded by [redacted] on Jul 2, 2012 • Last modified by [redacted] on May 12, 2020
Version 7

COMPLETE PROCESSING OF THE REQUEST SUBPROCESS [redacted] | May 12, 2020

IANA FUNCTIONS OPERATOR/RZM
Start
1.Update WHOIS
2.Have the public contacts or emails changed?
Yes
No
3.Was a new ticket created for RZMS credential changes?
Yes
No
4.Create new ticket in RT
5. Update RZMS credentials for the changed contacts/emails.
6.Notify new contacts of their user names or their access to manage the new domain
7.Metadata needed?
Yes
No
8.Add Metadata for new gTLD
9.Do IDN tables need to be removed?
Yes
No
10.Remove IDN tables
11.Do reports need to be published?
Yes
No
12.Publish Report
13. Merge any tickets with original request
End

Complete Processing of the Request Sub-process

Overview:

This sub-process describes the steps that RZMS/IANA Services Staff takes to complete processing of the root zone request.

1.	Update WHOIS
Description	RZM automatically updates the WHO S database with the requested changes
Actor	RZMS
Documents	RZMS admin interface: [redacted]
Steps	Update the ANA WHO S database with the requested changes Go to **Step 2.**

2.	Have the public contacts or emails changed?
Description	Were there changes to the public emails or contacts?
Actor	IANA Serv ces Staff
Documents	RZMS admin interface: [redacted]
Steps	Verify if there were changes to the public emails f yes go to **Step 3.**

	f no go to **Step 7.**

3.	**Was a ticket created in RT for RZMS credential changes?**
Description	s there a new ticket for the credential changes?
Actor	IANA Serv ces Staff
Documents	RT [redacted] RZMS admin interface: [redacted]
Steps	Verify if there is already a new ticket created for the RZMS credential change f yes go to **Step 5.** f no go to **Step 4.**

4.	**Create new ticket in RT**
Description	ANA Services staff creates a new ticket in the RT system
Actor	IANA Serv ces Staff
Documents	RT [redacted]
Steps	Create new ticket in RT regarding the RZMS credential change if needed Go to **Step 5.**

5.	**Update RZMS credentials for the changed emails**
Description	ANA Services staff updates RZMS with new credentials
Actor	IANA Serv ces Staff
Documents	RT [redacted] RZMS admin interface: [redacted]
Steps	Log into RZMS to update credentials for the new email addresses Go to **Step 6.**

6.	**Notify new contacts of their user names or access to manage domain**
Description	ANA Services staff notifies the new contacts of their user names or access to manage domain
Actor	IANA Serv ces Staff
Documents	RZM admin interface: [redacted] RT [redacted]
Steps	Send an email to the TLD contacts notifying them of their user names Go to **Step 7**

7.	**Metadata needed?**
Description	Does metadata need to be added?
Actor	IANA Serv ces Staff
Documents	RT [redacted] RZMS admin interface: [redacted]
Steps	This step only applies to new gTLD delegation requests f it is a new gTLD delegation request then metadata needs to be added f yes go to **Step 8.** f no go to **Step 9.**

8.	**Add Metadata for new gTLD**
Description	ANA Services staff adds the metadata for the new gTLD
Actor	IANA Serv ces Staff

Documents	[redacted]
Steps	Log in to [redacted] Under "Domains" click "add" Fill in "A lable" "Domain Type" "Status" and "Eligibility" Click "Save" Go to **Step 9.**

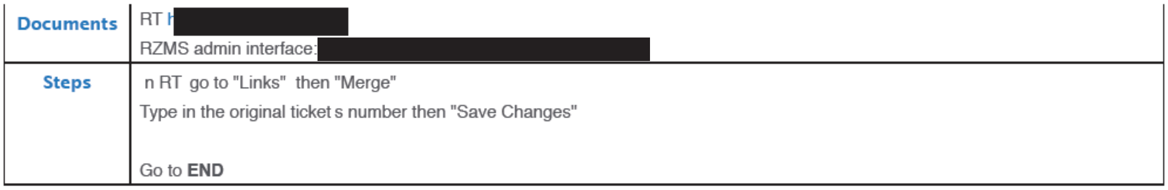
9.	**Do IDN tables need to be removed?**
Description	Are there are DN tables that need to be removed?
Actor	IANA Serv ces Staff
Documents	ANA Repository of DN Practices
Steps	This step only applies to revocation requests All DN tables need to be removed after a revocation request is completed f yes go to **Step 10.** f no go to **Step 11.**

10.	**Remove IDN Tables**
Description	ANA Services Staff removes DN tables
Actor	IANA Serv ces Staff
Documents	RT [redacted] ANA Repository of DN Practices RZMS admin interface: [redacted]
Steps	Determine if DN tables exist by going to https://www iana org/domains/idn tables Write a message in ticket to subject matter expert asking for DN tables to be removed Go to **Step 11.**

11.	**Do reports need to be published?**
Description	Do any reports needs to be published?
Actor	IANA Serv ces Staff
Documents	RT [redacted] RZMS admin interface: [redacted]
Steps	Confirm if there are still reports that need to be published Reports need to be published for delegation transfer and revocation requests f yes go to **Step 12.** f no go to **Step 13.**

12.	**Publish report**
Description	ANA Services staff publishes reports
Actor	IANA Serv ces Staff
Documents	RT [redacted] RZMS admin interface: [redacted] ANA Reports
Steps	Write a message in ticket to subject matter expert asking for report be published Make sure to either include the XML or PDF files which contain the report or refer to the original ticket Go to **Step 13**

13.	**Merge any tickets with original request**
Description	ANA Services staff merges related tickets with the original request ticket
Actor	IANA Serv ces Staff



Documents	RT [redacted] RZMS admin interface: [redacted]
Steps	n RT go to "Links" then "Merge" Type in the original ticket s number then "Save Changes" Go to **END**