

# User Documentation on Delegating and Redelegating a Country-Code Top-Level Domain (ccTLD)

## Table of Contents

<b>User Documentation on Delegating and Redelegating a Country-Code Top-Level Domain (ccTLD)</b> .....	<b>1</b>
<b>Delegating or redelegating a country-code top-level domain (ccTLD)</b> .....	<b>2</b>
Background on the process .....	2
Who is involved? .....	2
Preparing a request .....	3
Submitting the request.....	5
After the request is received .....	5
<b>Delegation Request Form</b> .....	<b>7</b>
<b>Technical requirements for authoritative name servers</b> .....	<b>9</b>
Definitions.....	9
Detailed requirements.....	9
Useful References.....	13
<b>Qualifying top-level domain strings</b> .....	<b>14</b>
Eligible categories of top-level domains .....	14
Eligible countries for country-code TLDs .....	14
<b>Preparing an Operational and Technical Plan</b> .....	<b>16</b>
General overview .....	16
Specific suggestions .....	16
On authoritative name server infrastructure .....	17
<b>Obtaining consent for a root zone change</b> .....	<b>19</b>
Standard confirmation .....	19
Consent from the Manager.....	19
Changes that impact multiple domains .....	19
<b>Common Questions on delegating and redelegating country-code top-level domains (ccTLDs)</b> .....	<b>20</b>

## Delegating or redelegating a country-code top-level domain (ccTLD)

This document provides an overall guide to the country-code top-level domain (ccTLD) delegation and redelegation process, and is designed to assist requestors in determining their eligibility, and in preparing formal requests.

### Background on the process

The delegation and redelegation process is designed to assign or re-assign a ccTLD to a manager, taking into account a number of technical and public interest criteria. These criteria relate to the basic principles that the manager be a responsible and technically competent trustee of the domain on behalf of the national and global Internet communities.

The process is initiated when a formal request is submitted to the IANA Root Zone Management staff at ICANN. The request and all required documentation is then reviewed and verified by these ICANN staff members. After the review and authorisations are completed, the request is implemented as a change to the Root Zone and Root Zone Database.

Upon successful completion of the process, the new country-code domain is established, or a transfer takes place in the case of redelegation of an existing ccTLD.

### Who is involved?

The delegation and redelegation process involves a number of different organisations and individuals. For example:

The **requestor**, usually the proposed manager, initiates the process by submitting a formal delegation or redelegation request. The requestor is the main party ICANN interacts with throughout the request, and is responsible for collecting much of the materials required to process the request.

The **proposed manager** is an organisation to which delegated responsibility for the ccTLD is sought. This organisation must demonstrate it understands and can meet its obligations as a trustee for the domain on behalf of the national and global Internet communities. The term manager is synonymous with other terms, such as Sponsoring Organization and operator, which have been used in other documentation. In this document, we have standardized on manager.

**Significant stakeholders** are those parties that benefit from the operation of the ccTLD, and their opinions are important in assessing the public interest aspects of a request.

The **respective government** is consulted to indicate either support or non-objection for the delegation or redelegation request. As a country-code represents the name of either a country or territory, the government is an important stakeholder in how the domain should be managed.

**ICANN**, as the IANA Functions Operator, is responsible for the receipt, verification and processing of the request. IANA Root Zone Management staff performs these activities.

The **U.S. Department of Commerce**, as the Root Zone Administrator, is responsible for verifying that processing procedures have been followed, and authorising any related changes to the DNS root zone and root zone database.

**Verisign**, as the Root Zone Maintainer, is responsible for receiving requests that have been processed by ICANN and authorised by the US Department of Commerce, implementing those changes in the root zone, and distributing the revised root zone to the root name servers.

While many parties are involved in processing a delegation or redelegation, the Root Zone Management staff at ICANN are the primary interface for those requesting a delegation or a redelegation of a ccTLD.

## Preparing a request

A delegation or redelegation request involves the development and submission of documentation that describes the nature of the request, and how the proposed new manager satisfies the criteria used to assess the request.

### Completing a delegation request form

The [delegation request form](#) which describes the basic details of the request, must be completed. The details include the identity of the proposed manager, the contact persons to be listed in the Root Zone Database, the technical delegation details for the domain, and a checklist relating to the assessment criteria for the delegation or redelegation request.

Please see “[Technical requirements for authoritative name servers](#)” for more information about the technical delegation details for the domain.

### Demonstrating string eligibility

To delegate or redelegate a ccTLD, it must be shown that the string is eligible to be delegated.

The primary method of eligibility for country-code top-level domains is its listing as an “alpha-2” (two-letter ASCII) code listed in the ISO 3166-1 standard. Another method of eligibility is the string may have been deemed eligible as a country-code through the IDN Fast Track process.

Complete details on which country-codes are considered eligible are available below in “[Eligible country-codes for delegation as a ccTLD.](#)”

### Demonstrating technical and administrative competency

The delegation request must include documentation that demonstrates the technical and administrative ability of the proposed manager to operate the domain competently and that they will not jeopardize nor compromise the stability and security of the DNS.

The proposed manager decides whom to list as the administrative and technical contacts. Both the administrative contact and the technical contact must cross-verify all root zone changes and be responsive to communications about root zone changes.

For more information on preparing documentation to demonstrate technical and administrative ability, please go to “[Preparing an Operational and Technical Plan.](#)”

## Providing information on the Proposed Manager

It is a requirement that the requestor provides the legal name of the organisation (as officially registered in its principal place of business), along with its physical address, telephone and fax numbers. In support of this, the requestor must provide a certified copy or extract of the business registration, certification, or law that demonstrates the organisation's legal status.

## Providing geographical location

As country-codes represent specific countries or territories, the proposed manager will be resident or incorporated in, the territory and/or jurisdiction of the relevant government or public authority of the country associated with the ccTLD, unless formally decided otherwise by the relevant government or public authority.

It is a requirement that the requestor indicate the geographic locations of the proposed manager, the administrative contact person for the domain, and the location(s) where the principal operations will be conducted.

## Demonstrating consent

It is a requirement that the requestor provides documentation that shows that directly involved parties consent to the request to delegate or redelegate. For a new delegation, this includes the proposed new organisation and contact persons. For an existing delegation, this also includes documented consent from the existing management of the domain.

## Demonstrating that the request serves the local Internet community's interest

The delegation or redelegation request must demonstrate that the proposed manager recognises its responsibility to fairly and equitably serve the local Internet community's interests with respect to management of the domain. In support of this, it is a requirement that the requestor document the mechanisms that will be utilised to inform and seek input from the local community on ccTLD management issues.

It is a requirement that the requestor provide documentation indicating local Internet community support for the proposed manager in operating the ccTLD, such as letters of support from interested and/or impacted parties, and the results of public consultations that led to the request.

## Demonstrating government review and consideration

It is a requirement that the requestor provide documentation indicating the relevant governments have been informed about the request. It is a requirement that the documentation includes a statement of support or non-objection from an authorised representative of the government.

## Demonstrating a stable transfer plan

For the redelegation of an existing operational ccTLD, it is a requirement that the requestor provide information on how existing operations will be transferred to the proposed new manager in a safe manner. It must explain how the stability of the domain will be preserved and how existing registrants will be impacted by the change. If the request is in relation to a transfer from a retired ccTLD to another ccTLD, it must also describe the decommissioning process for the retired domain.

## Submitting the request

Once the request has been prepared, submit it to ICANN's Root Zone Management staff to commence processing.

### Initial email submission

To start the request, send an email with the delegation/redelegation form attached to:

root-mgmt@iana.org

Supporting documentation must be provided with the [Delegation Request Form](#). Files should be in PDF format where possible.

Once the email is sent to root-mgmt@iana.org, ICANN's ticketing system will reply automatically with a confirmation of receipt and a unique reference number within 1 day. This number will be used to track progress and correspondence relating to the request. Please ensure the number, just as it appears in the confirmation receipt, is included in the subject of all future communications related to the request.

### Original documentation

In addition to the electronic submissions, it is a requirement that the requestor submit originals, or certified copies, of all official documents and testimony used in the request for which its authenticity is material to the evaluation. This includes the following:

- Registration certifications
- Letters of support or consent
- Legal documents that are a basis of the application

The documents should be couriered or posted to ICANN's Root Zone Management staff at the following address. It is important that the documents cite the reference number that appeared in the email confirmation receipt.

Root Zone Management  
ICANN  
12025 Waterfront Drive #300  
Los Angeles CA 90094  
USA

Please submit all requests, templates, and documentation in English. Where accuracy is essential, English documentation and/or English translations of key documents (such as governmental decrees relating to the request) must be notarised or certified official translations.

## After the request is received

Once we receive the request and issue a confirmation receipt, a process of analysis and verification begins. The amount of time this process takes varies depending upon the information provided in the supporting documentation, and the complexity of the individual case.

In the event that further documentation or clarification is needed, we will contact the requestor. The delegation or redelegation request will not proceed until we have received satisfactory documentation and information.

If we are unable to process the request due to significant lack of detail, the inability to confirm information, and/or unresponsiveness by the requestor, we will administratively close the request. In such cases, the requestor is welcome to resubmit the request at a later date to restart the review process once the additional material is available.

### Requesting confirmation from contacts

In addition to verification and analysis of the material supplied in the request, for redelegation requests, we will ask the current administrative and technical contacts, and the current ccTLD manager, whether they agree to the request.

In the case of a delegation, ICANN confirms with the proposed contacts as listed in the request, to ensure they consent to the responsibilities of being listed as a contact for the domain.

In those cases where confirmation is not received from one or more parties, further consultation will be necessary. This may delay processing of the request. Please see “[Obtaining consent for a root zone change](#).”

### Posting the status of the pending request

ICANN will publicly post requests for delegations and redelegations. This public disclosure will at a minimum include the domain name being requested, the party that will manage the domain, and the current status of the request.

If there are specific stability or security reasons why information should not be disclosed, the requestor should explain that in the [Delegation Request Form](#).

### Analysing the request

After all materials are received, and the positions of the contacts have been ascertained, ICANN staff performs an analysis of the request.

The result of this analysis is a report that describes how the application meets the various criteria. This report will be reviewed by the ICANN Board of Directors to confirm proper procedures were followed.

### Implementing the request

After the review by the ICANN Board, ICANN, as the IANA Functions Operator will forward the completed request to the Root Zone Administrator. The Root Zone Administrator will then authorize changes to the DNS root zone and root zone database. Upon authorization, the Root Zone Maintainer will implement the changes to the DNS root zone. The IANA Functions Operator will implement the data changes in the WHOIS database.

After the request has been implemented, we will notify the requestor, and the requestor will verify that the changes were made correctly. In the event any problems arise, immediately notify us at [root-mgmt@iana.org](mailto:root-mgmt@iana.org) and include the reference number of the change request.

## Delegation Request Form

This is to be used as part of submitting a delegation or redelegation of a country-code top-level domain.

IANA TLD MODIFICATION TEMPLATE 2010-02-17

\*\* This should be completed and submitted to [root-mgmt@iana.org](mailto:root-mgmt@iana.org).  
\*\* In most cases, this can be completed online. For more information  
\*\* visit <http://www.iana.org/domains/root/> or contact IANA for  
\*\* assistance.

1. Top-Level Domain Name.....:

2. Purpose of change.....:

### Manager

3a. Organisation Name.....:

3b. Street Address.....:

3c. City.....:

3d. State.....:

3e. Postal Code.....:

3f. Country Code (2 letter).....:

### Administrative Contact

4a. Contact Person's Name.....:

4b. Job Title.....:

4c. Organisation Name.....:

4d. Street Address.....:

4e. City.....:

4f. State.....:

4g. Postal Code.....:

4h. Country Code (2 letter).....:

4i. Phone Number.....:

4j. Fax Number.....:

4k. Email Address.....:

4l. Treat as role acct? (y/n).....:

### Technical Contact

5a. Contact Person's Name.....:

5b. Job Title.....:

5c. Organisation Name.....:

5d. Street Address.....:

5e. City.....:

5f. State.....:

5g. Postal Code.....:

5h. Country Code (2 letter).....:

5i. Phone Number.....:

5j. Fax Number.....:

5k. Email Address.....:

5l. Treat as role acct? (y/n).....:

### Authoritative Name Server

6a. Hostname.....:

6b. IP Address(es).....:

Authoritative Name Server (duplicate for additional name servers)

6a. Hostname.....:

6b. IP Address(es).....:

Delegation Signer Record (for DNSSEC signed zones only)

7a. Key Digest.....:

7b. Key Tag.....:

7c. Key Algorithm.....:

7d. Key Digest Type.....:

Delegation Signer Record (duplicate for additional DS records)

7a. Key Digest.....:

7b. Key Tag.....:

7c. Key Algorithm.....:

7d. Key Digest Type.....:

Domain Information

8a. URL for Registration Services...:

8b. WHOIS Server.....:

Special notes (for staff processing change, does not appear publicly)

9. Notes.....:

## Technical requirements for authoritative name servers

This document describes the baseline technical conformance criteria for authoritative name servers. These are evaluated by ICANN as the IANA functions operator for changes to delegations in the DNS root zone.

### Definitions

1. For purposes of this document, an authoritative name server is a DNS server that has been designated to answer authoritatively for the designated zone, and will be listed in the delegation. It is recorded by its fully-qualified domain name, along with its IP addresses.
2. Name server tests are completed against each unique tuple of a hostname, an IP address, and a protocol. If a hostname has multiple IP addresses, for example, the tests will be conducted against each IP address.

### Detailed requirements

#### Minimum number of name servers

There must be at least two NS records listed in a delegation, and the hosts must not resolve to the same IP address.

#### Valid hostnames

The hostnames used for the name servers must comply with the requirements for valid hostnames described in RFC 1123, section 2.1.

#### Name server reachability

The name servers must answer DNS queries over both the UDP and TCP protocols on port 53. Tests will be conducted from multiple network locations to verify the name server is responding.

#### Answer authoritatively

The name servers must answer authoritatively for the designated zone. Responses to queries to the name servers for the designated zone must have the “AA”-bit set.

The test to confirm this queries for the SOA record of the designated zone with no “RD”-bit set.

#### Network diversity

The name servers must be in at least two topologically separate networks. A network is defined as an origin autonomous system in the BGP routing table. The requirement is assessed through inspection of views of the BGP routing table.

#### Consistency between glue and authoritative data

For name servers that have IP addresses listed as glue, the IP addresses must match the authoritative A and AAAA records for that host.

## Consistency between delegation and zone

The set of NS records served by the authoritative name servers must match those proposed for the delegation in the parent zone.

---

## Consistency between authoritative name servers

The data served by the authoritative name servers for the designated zone must be consistent.

All authoritative name servers must serve the same NS record set for the designated domain.

All authoritative name servers must serve the same SOA record for the designated domain.

If for operational reasons the zone content fluctuates rapidly, the serial numbers need only be loosely coherent.

## No truncation of referrals

Referrals from the parent zone's name servers must fit into a non-EDNS0 UDP DNS packet and therefore the DNS payload must not exceed 512 octets.

The required delegation information in the referral is a complete set of NS records, and the minimal set of requisite glue records. The response size is assessed as a response to a query with a maximum-sized QNAME.

The minimal set of requisite glue records is considered to be:

One A record, if all authoritative name servers are in-bailiwick of the parent zone; and,

One AAAA record, if there are any IPv6-capable authoritative name servers and all IPv6-capable authoritative name servers are in-bailiwick of the parent zone.

For more information, see [Understanding packet size limits on DNS responses](#).

## Prohibited networks

The authoritative name server IP addresses must not be in specially designated networks that are either not globally routable, or are otherwise unsuited for authoritative name service.

---

0.0.0.0/8	Not globally routable	RFC 6890
<hr/>		
10.0.0.0/8	Not globally routable	RFC 6890
<hr/>		
100.64.0.0/10	Not globally routable	RFC 6598
<hr/>		

127.0.0.0/8	Not globally routable	RFC 6890
169.254.0.0/16	Not globally routable	RFC 6890
172.16.0.0/12	Not globally routable	RFC 6890
192.0.2.0/24	Not globally routable	RFC 6890
192.88.99.0/24	6to4	RFC 3068
192.168.0.0/16	Not globally routable	RFC 6890
198.18.0.0/15	Not globally routable	RFC 6890
198.51.100.0/24	Not globally routable	RFC 5737
203.0.113.0/24	Not globally routable	RFC 5737
224.0.0.0/3	Not globally routable	RFC 6890
::/128	Not globally routable	RFC 5156
::1/128	Not globally routable	RFC 5156
::FFFF:0:0/96	IPv4 mapped addresses	RFC 4291

2001:2::/48	Not globally routable	RFC 5156
2001::/32	Teredo	RFC 4380
2001:10::/28	Not globally routable	RFC 5156
2001:DB8::/32	Not globally routable	RFC 5156
2002::/16	6to4	RFC 3056
FC00::/7	Not globally routable	RFC 5156
FE80::/10	Not globally routable	RFC 5156

### No open recursive name service

The authoritative name servers must not provide recursive name service. This requirement is tested by sending a query outside the jurisdiction of the authority with the “RD”-bit set.

### Same source address

Responses from the authoritative name servers must contain the same source IP address as the destination IP address of the initial query.

### DS record format

Trust anchors must be provided each with the four attributes of a DS record — the key tag, the key algorithm, the digest hash type, and the digest hash. They must be provided with legal values for each of the DS record fields. For the hash digest, ICANN supports two types — SHA1 (value 1), and SHA256 (value 2).

## Matching DNSKEY

At the time of the listing request, there must be a DNSKEY that matches the DS record present in the child zone. This will be tested for as part of the implementation of the record. As with most technical conformance criteria for the root zone, if a top-level domain operator has a situation where this is not the case, but this is by design and can be demonstrated not to affect the stability of the TLD or the root zone, it is possible to request that the DS records be listed regardless.

## Validation of RRSIG

ICANN must be able to validate the RRSIG records returned for the zone based upon the DS record set that has been provided for the root zone. We test this by querying the apex SOA for the top-level domain with the DO bit set, and validating the SOA record against the proposed DS resource set.

## Useful References

For more information on some of the key DNS technical concepts referenced by these technical tests, please look at the following references:

- Domain Names — Concepts and Facilities (RFC 1034)
- Domain Names — Implementation and Specification (RFC 1035)
- Preventing Use of Recursive Nameservers in Reflector Attacks (RFC 5358)
- Operational Considerations and Issues with IPv6 DNS (RFC 4472)
- Extension Mechanisms for DNS (EDNS0) (RFC 2671)
- DNS Referral Response Size Issues
- DNS Transport over TCP - Implementation Requirements (RFC 5966)
- IANA IPv6 Special Purpose Address Registry
- Special-use IPv6 Addresses (RFC 5156)
- Special-use IPv4 Addresses (RFC 5735)

## Qualifying top-level domain strings

### Eligible categories of top-level domains

The current ways in which a top-level domain can be eligible for delegation are as follows:

Approved generic top-level domain. The domain needs to have been successfully reviewed and completed the evaluation and contracting process with ICANN to be a generic top-level domain.

ISO 3166-1 alpha-2 code. The two-letter (“alpha-2”) code that is assigned in the ISO 3166-1 standard is eligible for delegation as a country-code top-level domain. This is the standard path of eligibility for ASCII country-code top-level domain strings.

IDN Fast-Track Approved String. The domain reflects a string that was approved by the ccTLD Fast-Track IDN process. The country for which the string was approved must continue to be listed in the ISO 3166-1 standard. If the country is no longer in the ISO 3166-1 standard, the string is no longer eligible for delegation.

Eligible under ICANN Board Resolution 00.74. This resolution provides for eligibility for domains that are not on the ISO 3166-1 standard, but that the Maintenance Agency deems exceptionally reserved, and requires that the Agency “has issued a reservation of the code that covers any application of ISO 3166-1 that needs a coded representation in the name of the country, territory, or area involved”. There is currently (as of June 2013) only one code eligible under these requirements, “EU” for the European Union.

Grandfathered prior to 2000. ICANN codified the rules under which future exceptionally reserved delegations may be considered in 2000 in Resolution 00.74. Certain domains were delegated on the basis of being “exceptionally reserved” by the ISO 3166 Maintenance Agency prior to this date. These domains were “.UK”, “.AC”, “.GG” and “.JE”. Of these, “.GG” and “.JE” are now listed in the ISO 3166-1 standard and therefore qualify normally. The remaining two domains that are grandfathered under their original eligibility are “.UK” and “.AC”.

Infrastructure domain. The domain “.ARPA” is delegated as a special “infrastructure” top-level domain for certain technical purposes, following procedures developed in the IETF and overseen by the Internet Architecture Board.

Test domain. According to Board Resolution 07.47, a series of test top-level domains are eligible for delegation for testing purposes. As of 2013, 11 top-level domains have been delegated according to this policy.

### Eligible countries for country-code TLDs

ICANN is not in the business of deciding what is and what is not a country. Instead, we employ a neutral standard maintained by the [ISO 3166 Maintenance Agency](#). Our policy is to create new country-code top-level domains when the country or territory is listed on the ISO 3166-1 standard.

The codes we use are two-letter codes from the [ISO 3166-1 standard](#). The selection of the ISO 3166-1 standard as a basis for country-code top-level domain names was made with the knowledge that ISO has a politically neutral procedure for determining which entities should be and should not be listed in the standard.

The ISO 3166-1 standard is a broadly accepted list of country-codes intended for many uses, not simply for use as country-code top-level domains. Accordingly, in [describing the relationship between the ISO 3166-1 list and ccTLDs](#), the ISO 3166 Maintenance Agency includes the following:

For quite some time now, individual persons or organisations interested in obtaining their “own” TLD have been requesting the inclusion of “new” country names into ISO 3166-1 in order to get a new alpha-2 code element from the ISO 3166/MA and subsequently a ccTLD from ICANN. Such requests are absolutely futile, however, because the only way to enter a new country name into ISO 3166-1 is to have it registered in one of the following two sources:

United Nations Terminology Bulletin Country Names or  
Country and Region Codes for Statistical Use of the UN Statistics Division

To be listed in the bulletin Country Names you must either be

a member country of the United Nations,  
a member of one of its specialized agencies or  
a party to the Statute of the International Court of Justice.

The list of names in the code of the UN Statistics Division is based on the bulletin Country Names and other UN sources.

Once a country name or territory name appears in either of these two sources, it will be added to ISO 3166-1 by default.

## Preparing an Operational and Technical Plan

This section provides additional detail on preparing an operational and technical plan as it relates to the procedure to delegate or redelegate a country-code top-level domain (ccTLD).

### General overview

ICANN's role is to review whether the proposed manager will perform its tasks with a satisfactory level of operational and technical competency. We primarily do this by asking a requestor to provide a technical and operational plan describing how the proposed manager will manage the domain.

It is recognised that the requirements for operating a ccTLD vary significantly by country. The operational approach for a small country with limited number of domains will be very different from a registry that maintains millions of registrations and has committed to providing a high-level of uptime, 24×7 support, and an automated registration interface such as an EPP-based registry.

The review process is not intended to enforce a particular approach on all requestors. We review the planning assumptions made against the proposed set up of the operation. We apply our understanding of industry norms, to consider if the assumptions are reasonable and if the proposed operation is likely to satisfy those assumptions. If the assumptions or plans appear unreasonable, we will make additional enquiries to the requestor to better understand the proposal.

Considering this assessment approach, a key part in developing a plan is documenting the assumptions and policy constraints that apply to the operation. For example, some of the questions to consider would be: What are the number of projected domains within the ccTLD that need to be managed? How many transactions are expected to be processed? What are the service-level obligations (for uptime, responsiveness, etc.) that the registry is committed to? What are the specific policy requirements that the registry is required to implement?

If the plans provided do not document such assumptions, or do not provide a sufficient level of detail so that the proposed operations can be understood, we may not be able to properly assess the technical and operational capacity of the proposed manager.

Requestors should be aware the plans are not just limited to the technical systems, but also to other resourcing of the proposed management of the domain. Plans should include explanations of the software, hardware, network architecture, staffing, expertise and facilities of the proposed manager.

### Specific suggestions

In light of the general advice, some of the specific elements the requestor should consider providing include:

- a) description of the organisation's structure, key personnel (financial and business officers, and other relevant management employees), and an overview of overall staffing;
- b) information on the proposed administrative and technical contacts for the domain, including their identities, contact details, and roles within the organisation;

- c) description of the proposed manager's relevant Internet management and registry operations experience;
- d) information on the technical capabilities of the manager, including the technical plan for registry and DNS operations, and a description of the physical configuration of the registry, along with technical facilities;
- e) assurance that relevant policies will be in place to govern the operation of the domain, as to not jeopardize or compromise the security and stability of the DNS;
- f) indication that security plans and procedures will be in place, including database and physical security for the operation of the domain;
- g) indication that plans exist to cope with the requirements of scaling registry operations as required;
- h) a description of the domain registration model, such as whether a registry-registrar model, or direct interaction with the registry;
- i) indication that the requesting organisation has sufficient Internet connectivity and services capable to provide connectivity, redundancy and resiliency;
- j) description of the configuration and plan for the name server constellation that will support name resolution for the domain;
- k) description of the registry's interfaces with the community (such as technical APIs, help desk, etc.), and how they will be maintained;
- l) information on how zone data will be generated and how public WHOIS services will be provided;
- m) information on resiliency provisions, including how system outages and other disasters will be defended against, as well as system recovery and escrow procedures in the event of disasters;
- n) indication that processes and plans are in place to ensure operations are in line with global standards, relevant RFCs, and best practices; and
- o) description of the timelines and strategies relating to deployment of the registry technical platform and staffing of the registry, if the registry is not already fully commissioned.

### **On authoritative name server infrastructure**

It should be assumed there is an expectation that the authoritative name service, as a whole, must always be available for any top-level domain.

The configuration of the name servers for a top-level domain should be sufficiently well designed to assure constant availability against any adverse event. This includes major denial-of-service attacks and unforeseen disasters in the country. Even though registration activity may be impaired by such events, the name server infrastructure should be designed such that the ability to resolve the top-level domain's zone should never be impacted.

Requestors should consider geographically and topologically diverse infrastructure that is not dependent on specific networks in order to achieve this goal. The advent of anycast-based approaches to name server deployment makes this more viable than it may have been in the past.

## **Obtaining consent for a root zone change**

### **Standard confirmation**

For a routine change to a top-level domain, the existing administrative and technical contacts should both consent to a change.

For changes that involve appointment of new contacts, the proposed new contacts will also be required to consent to the change. They will be asked to confirm their details are correctly reflected and they agree to the responsibility of being a contact for the domain.

### **Consent from the Manager**

In the event either the administrative or technical contact is unresponsive, or it can be shown they no longer act in the role for which they were designated, the manager is able to provide instruction regarding authorising changes or replacing the contacts. This should be provided by an appropriately authorised representative of the manager, on company letterhead. We will confirm the authenticity of the communication before proceeding with the change request.

### **Changes that impact multiple domains**

If a change involves altering the IP address(es) for a name server, and that name server is used by two or more top-level domains, confirmations from the contacts of the other impacted top-level domains must be provided.

After 14 days, if such a request is consented to by the requesting domain's contacts, but is stalled because not all of the other impacted parties have explicitly consented, we may apply discretion to proceed with the request. Note that if any party explicitly rejects the request, the request will be closed.

## **Common Questions on delegating and redelegating country-code top-level domains (ccTLDs)**

### **How long does a delegation/redelegation request take?**

Every delegation or redelegation request is different. With many organisations participating in any particular request, the processing can be affected by delays in coordinating and communicating among the parties, obtaining the necessary approvals, and verifying the information provided. The process is further complicated when not all parties agree to the request.

Because of this, it is not possible to predict an accurate timetable for the process from receipt of the request through to completion. Fully-formed requests that clearly meet all relevant criteria can take as little as 1-2 months. In some extreme and complicated cases, requests have sometimes taken a number of years.

### **When in the process should a redelegation request be submitted?**

The request to redelegate a ccTLD should be submitted once the requestor knows the proposed new manager of the ccTLD, and has plans on how the ccTLD will be operated, but prior to any transfer taking place. The transfer of operations to the new manager happens once a redelegation request has been approved.

It is OK to contact ICANN prior to submitting a formal request to better understand the procedure, or to give ICANN early notice of work being done in the country on a redelegation. It is better if ICANN is able to assist the requestor early on to understand the redelegation process to avoid misunderstandings that could delay transition later.

### **If a company runs an existing ccTLD, can it provide less documentation for a delegation or redelegation request?**

Generally, the documentary requirements are the same for a new request, regardless of whether the proposed manager operates an existing ccTLD or not. In particular, the requirements of the process are more formalised than they were in the 1980s and 1990s when the bulk of existing ccTLDs were first delegated. A successful request for delegation in the 1980s does not imply that a request would necessarily be successful again under contemporary criteria. As such, ICANN will review new requests under the existing procedures without any assumptions about why a delegation qualified at an earlier time.

It should be noted that a successful history in operating existing TLDs may form an important part of documenting the operational and technical skills of the proposed manager.

### **If a company simply changes its name, does it need to complete a full redelegation request?**

There are some special cases where a change to the manager may be deemed to not be a material change to the organisation. In such cases, the change can be considered an “administrative redelegation”, which means that it can be considered a routine update rather than requiring an evaluation of the new manager.

ICANN will check if a change request to a manager reflects a change of administrative responsibility to a new organisation that is essentially the same as the previous organisation.

These situations are typically where ccTLD management has shifted as the result of an internal restructuring, internal governmental restructuring, or the organisation has simply changed its name.

In such cases, to be considered non-material, day-to-day operations must remain unaltered. For example, there would normally need to be continuity of staff, policy, policy setting structure, levels of service, legal character and so on.

When a request is deemed non-material, ICANN will process the request as a regular root zone change request, rather than as a delegation request. If there is any doubt, the full redelegation process will be used to fully investigate the nature of the change.

If ICANN considers a request to be eligible an administrative redelegation, it will advise the requestor.

### **If a registry's technical operations are outsourced to a company, what organisation should be the Manager?**

If an organisation that sets and administers policy for the ccTLD outsources the back-end technical operation of the ccTLD to another company, typically it is the policy organisation that is listed as the Manager. If the technical outsource operator is the right party to contact for technical enquiries for the domain, that party could be listed as a Technical Contact.

### **Does the government need to be consulted on a request?**

As an important part of the local Internet community, it is expected that relevant local governments are consulted regarding a delegation or redelegation. It is not a requirement they consent, but if they do not have an opinion, a statement of non-objection can be useful.

If the government is non-responsive, the requestor should provide clear evidence they made reasonable attempts to discuss the request with relevant government representatives.

### **What are the local presence requirements?**

For each ccTLD, at a minimum both the manager and the administrative contact must be resident in the country to which the domain is designated. This means they are accountable to the local community and subject to local law.

For sub-national territories, it is considered acceptable (with the consent of the local Internet community) if the manager and the administrative contact are located elsewhere in the country so long as they are still subject to applicable law.

### **What should be in a letter of endorsement from a government?**

When communicating support for a delegation or redelegation by a government representative, there are no strict formatting requirements, but ICANN recommends the letter reference the following points:

An explanation why the agency or author is the appropriate representative of the government to be providing support.

If the support reflects formal decision-making made under the powers granted by a specific law or regulation that covers the ccTLD, that law or regulation should be cited. It should be clear that the decision is made under the powers of the specific law or regulation.

Clearly express the position — whether it is approving of the proposed request, not approving of the proposed request, or expressing non-objection to the request.

Refer to the IANA-assigned ticket number (if available) and identify clearly the specific organisation and circumstances under which the position is being supplied. This is to avoid a scenario where it is unclear which organisation or which request the communication is referring to.

## **Is it appropriate for a regulator to be the Manager?**

The relevant frameworks, including the delegation assessment procedures, call for the Manager to actively be responsible for the operation of a ccTLD. If a regulator runs the domain registry itself, and all other criteria are satisfied, then it would be appropriate for the regulator to be the Manager for the ccTLD.

## **Does the government or regulator have to be the manager to have involvement in deciding how the domain is operated?**

It is not necessary for a government or regulator to be a manager for a ccTLD as a mechanism for them to have a say in how the domain is operated. Governments are consulted for all redelegation requests for the domain regardless of whether they are listed in the record (see the GAC Principles). Furthermore, the manager is required to be located within the country and to comply with local laws.

## **How does a requestor demonstrate local Internet community support?**

The Manager for a ccTLD is considered a trustee on behalf of the local community in the country. Some of the elements that could show support for the request are:

**Community consultation.** It is typically an important aspect of selecting the proper manager for a ccTLD to consult with the local Internet community. Providing documentation that shows which consultations were performed, who was able to participate in them, and that participation was broadly representative of the community is one good way to show a bottom-up process was used to arrive at the proposal for the new manager. Relevant documentation might include timelines, minutes of meetings, pointers to online consultations and compilations of feedback received.

**Describe the options considered.** It is rare there is a uniform agreement that a particular approach is the best approach. It is helpful to document what alternatives have been considered regarding management of the ccTLD, what the pros and cons of the options were, and how those considerations were factored into the final decision. If there is opposition to the request, it is useful to document that.

**Statements of support.** Expressions of support from representatives of the local Internet community can also be helpful in describing local support for the application. (See [What should be in a statement of support or objection from an interested party?](#))

## **What should be in a statement of support or objection from an interested party?**

When communicating support for a delegation or redelegation by an interested party, there are no strict formatting requirements, but ICANN recommends the letters reference the following points:

Explain the person or organisation providing the statement, and what their role is in the local Internet community. If the organisation is a representative organisation, explain the membership or community sector the organisation is representing.

Clearly express the position — whether it is approving of the proposed request, not approving of the proposed request, or expressing non-objection to the request.

Articulate the reasons why the organisation is considered appropriate or not appropriate for managing the ccTLD on behalf of the local Internet community.

Provide an explanation of the alternatives that have been considered, and why this proposal is their preferred or non-preferred option.

It is less useful if the statements are merely “form letters”, where multiple organisations provide letters that are comprised of the same language that has been drafted for them by the requestor. Each communication should uniquely represent the views of that specific party.

## **Must originals of all documents be submitted?**

ICANN only needs originals (or copies that have been properly certified as accurate) for documents where the authenticity is important to the validity of the request. This means items such as certifications, extracts of relevant laws and decrees, and letters of support. ICANN needs to independently verify these kinds of documents as authentic with third parties.

ICANN does not need copies of documents such as operational or technical plans. They can be provided as PDF files electronically to us, but the requestor does not need to send them to ICANN by post.

## **Do all documents need to be provided in English?**

Generally, ICANN needs all documentation to be provided in English, or be certified translations into English. For complex or long documents (such as complete legislative acts), it is generally OK to only translate the relevant portions.

In some cases, if there are particular difficulties in providing translations, a requestor should talk with ICANN’s Root Management staff, who will help find a workable approach. While ICANN does have capacity to translate certain types of documents, the process of getting certified translations can introduce significant delay in processing a request.

## **What is the process for retiring a country-code top-level domain?**

When a ccTLD is no longer eligible, typically due to the country or code’s removal from the ISO 3166-1 standard, the operator is expected to develop a transition plan to the successor ccTLD(s) and ultimately retire the domain. Consistent with the general approach that ccTLDs are to be managed within the country, the manager is expected to design and execute a locally-appropriate

method of notifying impacted registrants that the domain is to be retired, and develop a timeline to transition to new ccTLDs.

This transition and retirement plan is reviewed in a similar fashion to a delegation or redelegation request. As countries are typically replaced with new successor countries, this process is usually performed in conjunction with delegation of new ccTLDs. Usually there is a transition period of several years so that there is plenty of time for registrants to transition to the new domain(s).

ICANN works with the manager to provide guidance and assistance throughout the whole process based on ICANN's experience from other countries that have had to perform a retirement transition.