28 March 2019

Guideline for Risk Mitigation Measures Evaluation

This Guideline details the risk mitigation measures evaluation process defined in Section 5.6.3 of the Final Implementation Plan for IDN ccTLD Fast Track Process (FIP) (as revised on 28 March 2019).

1 Introduction

As per IDN ccTLD Fast Track Process Implementation Plan (hereafter: FIP), a selected IDN ccTLD string should not be confusingly similar with (i) any combination of two ISO 646 Basic Version (ISO 646-BV) characters (letter [a-z] codes), nor (ii) existing TLDs or reserved names.

To evaluate possible confusing similarity in the IDN ccTLD Fast Track process, ICANN organization has appointed the following two panels:

- **DNS Stability Panel (DSP).** The DSP conducts the initial DNS Stability Evaluation, which includes a string similarity review of the requested IDN ccTLD string.
- **Extended Process Similarity Review Panel (EPSRP).** The EPSRP conducts a review of the requested IDN ccTLD string for contention cases identified by DSP upon the request of the requester, using the same criteria but with a different methodology from DSP[1].

In 2019 Section 5.6.3 of the FIP has been updated to introduce the evaluation of mitigation measures to reduce risks associated with confusingly similarity of TLD strings. This describes the process on how to propose and review mitigation measures.

2 High Level Overview Risk Treatment Appraisal Process

At the request of the requester of an IDN ccTLD string and under the eligibility conditions of this guideline, the Risk Treatment Appraisal Process Panel (RTAP Panel) will need to be satisfied that the proposed risk mitigation measures are adequate and the requester has followed an appropriate risk management process.

Should the RTAP Panel have concerns as to the adequacy of the proposed mitigation measures or the proposed risk management process, the RTAP Panel will communicate with ICANN and the requester during the process to understand the objective and the Risk Mitigation Proposal (RMP), and the requester may provide additional information and clarification.

Based on the inputs and analysis, RTAP Panel will determine whether the proposed risk mitigation measures are adequate.

3 Conditions for Applying these Guidelines

In accordance with section 5.6.3 of FIP and under the following limited set of conditions, a requester is eligible to propose measures to mitigate the risk associated with confusing similarity:

- If the DSP or EPSRP evaluation has determined that the requested string is confusingly similar in uppercase only (and not in lowercase).
- The requester has filed a request for a review of its proposed mitigation measures within three months from the date the results from the DSP and/or EPSRP have been communicated to the requester or, if at a later date, within 3 months after the date at which this guideline becomes effective.
- In the request for a review of proposed mitigation measures, the requester has included, at a minimum, proposed mitigation measures and a reference to the proposed,

[1] Following the methodology in its guidelines, for the scripts which are bicameral the EPSRP provides separate recommendations for uppercase and lowercase versions of the requested IDN ccTLD strings given that from a visual similarity point of view, uppercase and lowercase characters of the same letter are distinct entities (see for example: https://www.icann.org/en/system/files/files/epsrp-greece-30sep14-en.pdf).

internationally recognized and appropriate risk management and mitigation process the requester intends to use.
- The requester commits to implement the proposed and agreed upon mitigation measures as of the moment the IND ccTLD becomes operational.

If the above conditions are met, the review and evaluation of the proposed mitigation measures and methodology shall be undertaken by an independent panel (the RTAP Panel), appointed by ICANN.

The RTAP Panel shall evaluate the proposed risk mitigation measures and the risk management process to assess whether the risk of confusing similarity identified by the DSP or the EPSRP evaluations has been mitigated.

4 Objective and Criteria of Review of Risk Mitigation Measures

The mitigation measures proposed in the RMP should meet the objective of Risk Mitigation Measures and the criteria for review of Risk Mitigation Proposal.

The requester should make clear how the risk management process and proposed mitigation measures contained in the RMP meet the objective and criteria and should be evaluated together with the confusability findings.

4.1 The Objective of the Review of Risk Mitigation Measures

The objective of the review is to determine if the risk is effectively treated by the mitigation measures, as per the statement below:

If a requested string has been found to be confusingly similar with the uppercase version of other strings, the proposed mitigation measures should reduce the risks associated with the confusing similarity to an acceptable level or threshold. The proposed mitigation measures should be evaluated in relation to the strings identified by the relevant panel (DSP or EPSRP) as confusingly similar to the applied-for string. In accordance with the IDN ccTLD Implementation Plan, the RTAP Panel should consider the likelihood of confusing similarity with specific consideration of confusability from the perspective that any domain name may be displayed in either upper- or lower-case, depending on the software application and regardless of the user's familiarity with the language or script. The residual level of risk, if any, due to the confusability of domain names is expected to be in the same range as which would occur by adding another IDN ccTLD which has not been found similar to existing or reserved TLD.

4.2 Criteria for Risk Treatment

The mitigation measures agreed by the applicant should be comprehensive, adequate, conservative and self-contained:

1. **Proportionate:** The mitigation measures will be in proportion to risks identified. The higher the risks, the greater the mitigation measures will be required; conversely, lower mitigation measures will be a proportionate response to risks that are identified as low severity or low likelihood.
2. **Adequate:** For each of the case(s), the measures should reduce the risk of user confusion arising from the potential use of the applied-for TLD to an acceptable level. The residual level of risk, if any, due to the confusability of domain names is expected to be in the same range as which would occur by adding another IDN ccTLD which has not been found similar to existing or reserved TLD.

3. **Self-contained:** The proposed mitigation measures can only apply to the registration policies of the applied-for TLD and do not assume any restrictions on the availability or registration policies of other current or future TLD labels.
4. **Global impact**: The proposed mitigation measures must have global applicability, and not only apply to confusability within the intended user community.

5 Risk Treatment Appraisal Process Panel (RTAP Panel)

Effective risk analysis and mitigation require expertise in the area of risk management and risk management processes and procedures. To guide the discussion and coordinate the assessment work and given the paramount nature of this kind of expertise, at least one person on the panel should be a recognized expert in this area.

The team doing the risk analysis should also include persons who are considered experts in the area of internationalized domain names, how related registration policies are implemented by the registries (to review the practicality of implementing the RMP), how IDNs may be confusing, to what extent such confusion can cause harm and how such confusion and harm could be prevented.

Therefore, the RTAP Panel will have three (3) to five (5) members, ensuring all the following requirements/skill sets are represented:

- Expertise in and understanding of various risk mitigating processes and standards and risk mitigation practices.
- Expertise on IDN implementation by registries, good understanding of the implementation opportunities and challenges for different IDN policies at the second and other levels, and knowledge of the relevant security and technical standards relating to IDNs.
- Expertise in brand protection, trade mark law and domain name disputes pertaining to the use of domain names as instruments for phishing and other sorts of abusive use, their impact and measures to address them.
- Expertise in the relevant language(s)/script(s).

ICANN organization convenes the RTAP Panel to review the anticipated RMP. The RTAP Panel members shall appoint one of their members to be the chair of the RTAP Panel.

The names of the members of the RTAP Panel will be listed on the ICANN website as soon as possible following their appointment and included in the report.

6 Risk Treatment Appraisal (RTA) Process

1. Requester submits the RMP within three (3) months after receiving the communication of the string similarity review decision[2]
2. ICANN organization convenes the RTAP Panel, and forwards RMP to RTAP Panel within one (1) week of the formation of the RTAP Panel

[2] For applications in the process before the implementation of these guidelines, this period will start from the date of publishing of the announcement that these guidelines are applicable.

3. The RTAP Panel creates a review plan within three (3) weeks for the completion of the work, which includes at a minimum:
    a. Tentative work plan and timeline
    b. Request, if any, for additional information which may be needed or helpful
4. ICANN organization reviews the RTAP Panel's evaluation plan, and informs the requester of the timeline and any additional information needed
5. Requester considers the review plan and shares any feedback, and additional information requested with respect to the RMP, and any other information considered necessary and /or relevant as soon as possible and confirms whether to proceed with the RTA.
    a. If the confirmation is not received within eight (8) weeks of receiving the review plan, the application is closed
6. ICANN organization forwards the updates with respect to the RMP, if any, to RTAP Panel, within one (1) week of receiving it
7. RTAP Panel undertakes analysis of the RMP. ICANN organization coordinates any additional interaction between RTAP Panel and requester with respect to any clarifying question RTAP Panel may have or additional information the requestor intends to provide with respect to the RMP
8. The RTAP Panel creates and hands over to ICANN organization a first RTA-Interim Report within eight (8) weeks of receiving the requester's confirmation to proceed with the RTAP
9. ICANN organization passes RTA-Interim Report to the requester within one (1 week) of receiving it
10. Requester submits its response and any additional information it considers relevant on the RTA-Interim Report and updated RMP (if at all) to ICANN organization within four (4) weeks of receiving the RTA-Interim Report
11. ICANN organization sends the response and updates of the RMP (if any) to RTAP from the requester. If requester has not submitted a response within four (4) weeks after receiving the Interim Report, ICANN will inform the RTAP Panel that they may continue to next steps
12. The RTAP Panel creates the RTA-Final Report and sends it to ICANN organization within (4) weeks of receiving the requester response on the RTA-Interim Report, or if no response is received within four (4) weeks of the expiry of the deadline for filing a response. ICANN organization coordinates any clarifying questions between RTAP Panel and the requester
13. ICANN organization sends the RTA-Final Report to the requester and publishes it one (1) week after sending it to the requester

6.1 Closure of process

The end result of the review process is either of the following options:

- A documented and consolidated recommendation from the RTAP Panel, following consultations with the requester, confirming that:
    - The requester has adopted an appropriate risk management methodology and framework;
    - The mitigation measures are proportionate and adequate to treat the risk(s) identified by the DSP or EPSRP (as the case may be);
    - The requester/ IDN ccTLD operator has committed to implement the mitigation measures prior to or on launch of the IDN ccTLD string(s);

- A documented and consolidated recommendation confirming the risk is not adequately treated, given the list of mitigation measures being proposed by the requester.

The end result of the review will be made public.

7 Risk Treatment Appraisal (RTA) Reports

There are two kind of reports generated by the panel. There is *RTA-Interim Report* which identifies gap(s) and (possibly) recommends any additional controls and solutions to mitigate risks identified. The second, the *RTA-Final Report* provides the final consolidated recommendation after evaluating the RMP by the requester. These reports would contain at least the following details.

7.1 RTA-Interim Report

1. *Objective and scope of the risk management process.*
2. *Summary of the external and internal context and how it relates to the system being assessed.*
3. *Summary of the methodology used for various stages of risk management.*
4. *Assessment of risk and breakdown of overall risk into its itemized component risks, with description of each component risk, the gap it causes, the end-user communities it impacts, and its evaluation.*
5. *Summary of the initial RMP by the requester, its break down into constituent controls, and how applicable constituent controls address each component risk.*
6. *Analysis of the degree (and description) of residual risk for each component risk after applying the proposed constituent controls.*
7. *For each component risk and in accordance with the objective and criteria set out in these guidelines, a detailed evaluation if the residual risk is still at significant level. Why? Why not?*
8. *Any suggestions, if available, for effectively addressing any of the residual risks which is still considered significant.*
9. *Based on the RMP, the residual risk for each component risk, what is the interim consolidated recommendation: is the cumulative risk effectively mitigated based on the RTA objective? Why? Why not?*

7.2 RTA-Final Report

1. *Objective and scope of the risk management process.*
2. *Summary of the external and internal context and how it relates to the system being assessed.*
3. *Summary of the methodology used for various stages of risk management.*
4. *Assessment of risk and breakdown of overall risk into its itemized component risks, with description of each component risk, the gap it causes, the end-user communities it impacts, and its evaluation.*
5. *Summary of the initial RMP, and any response or changes to the mitigation measures proposed by the requester in response to the RTA-Interim report,*
6. *Summary of the final RMP, its break down into constituent controls, and how applicable constituent controls address each component risk.*
7. *Analysis of the degree (and description) of residual risk for each component risk after applying the proposed constituent controls.*

8. *For each component risk, and in accordance with the objective and criteria set out in this guideline, a detailed evaluation if the residual risk is still at significant level. Why? Why not?*
9. *Based on the RMP, the residual risk for each component risk, what is the final consolidated recommendation: is the cumulative risk effectively mitigated based on the RTA objective? Why? Why not?*

Glossary

- Risk Mitigation Proposal, by the requester – RMP. The RMP should include at a minimum the proposed internationally recognized and appropriate risk management and mitigation process the requester has used and intends to use, and the proposed mitigation measures.
- Risk Treatment Appraisal - RTA
- Risk Treatment Appraisal process - RTAP
- Risk Treatment Appraisal Process Panel – RTAP Panel (none DRP EPSPR or ICANN employees or contractors)

8 Process Flow Diagram