ICANN

Los Angeles Headquarters

12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536
USA

☎ +1 310 301 5800

+1 310 823 8649

15 December 2017

RE: Implementing ICANN Board Resolution on Refinement of Similarity Review

Katrina Sataki, Chair, ccNSO, and
Patrik Fältström, Chair, SSAC

Dear Katrina Sataki and Patrik Fältström,

As per the information provided to ccNSO and SSAC in the letter dated 6 December 2017 (see https://www.icann.org/en/system/files/correspondence/atallah-to-sataki-faltstrom-06dec17-en.pdf), please find attached the initial draft of the guidelines developed by the ICANN organization to evaluate the risk mitigation measures proposed by applicants in the IDN ccTLD Fast Track process.

We request the pertinent working party of the ccNSO and the SSAC to review these guidelines and provide appropriate feedback to guide us to align these guidelines with the Joint ccNSO SSAC Response to ICANN Board on EPSRP.

We thank you for your consideration and look forward to the feedback.

Best regards,

Sarmad Hussain

Sarmad Hussain
Director, IDN Programs

<date>

Guidelines for the Appraisal of Risk due to String Similarity and its Mitigation in the IDN ccTLD Fast Track Process

These Guidelines provide details of the process to propose and evaluate the risk mitigation measures described in Section 5.6.3 of the Final Implementation Plan for IDN ccTLD Fast Track Process (FIP) (as revised on <date>).

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 of the requested IDN ccTLD strings in the Fast Track process, ICANN organization has appointed the following two panels:

- **DNS Stability Panel (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),** conducts a review of the applied-for IDN ccTLD string for contention cases identified by DSP upon the request of the applicant, using the same criteria but with a different methodology from DSP[1].

Both the DNS Stability Panel and the EPSRP evaluate confusability without taking into account any mitigation measures.

2 Conditions for Applying these Guidelines

Following latest update of the FIP, a subsequent step in the process allows for risk mitigation measures to be considered, under the following limited set of conditions:

- The starting point for the analysis are the results from the DSP or the EPSRP evaluations.
- Only for the bicameral scripts and only when a string is found confusingly similar in uppercase (and not in lowercase), allow the requestor to suggest mitigation measures that take into account the various conditions (varying display of the string in different software applications and varying level of the user's familiarity with the language or script).
- The applicant has to propose mitigation measures and request their review within three months from the date the string similarity results have been communicated to the applicant.
- Review of the suggested mitigation measures results in one of the following two possible outcomes, which will be made public (as per the details in Section 8 below):
  - A consolidated recommendation confirming that the risk is adequately treated, along with the list of mitigation measures agreed upon by the applicant/ IDN ccTLD operator.
  - A consolidated recommendation confirming the risk is not adequately treated, given the list of mitigation measures being proposed by the applicant.

The goal is to reduce the potential risk of user confusion as of the moment the IDN ccTLD becomes operational, including specific consideration of confusability from the perspective that any domain name may be displayed in any case (lowercase or uppercase). This guideline specifies the process and methodology for review of the mitigation measures.

3 Terms Used

- Risk Mitigation Proposal by the applicant - RMP
- Risk Treatment Appraisal - RTA

[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 applied-for IDN ccTLD strings as it believes that from a visual similarity point of view, uppercase and lowercase forms of the same letter are distinct entities.

- Risk Treatment Appraisal Panel - RTAP

4 Objective of 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:

> *In case the applied-for IDN ccTLD becomes operational after implementing the risk mitigation measures agreed by the applicant, the security and stability risk for end-users globally caused by the possible creation of confusable domain names in uppercase or lowercase is no more than the risk due to the confusability of domain names which would occur by adding another IDN ccTLD which has not been found similar to existing or reserved TLD labels by DSP or EPSRP. In case of reserved labels not operational at this time but found similar with the applied-for IDN ccTLD (e.g. from {aa…zz}), the confusability should be considered in the context that such TLD labels may become operational in the future without any restrictions.*

5 Risk Treatment Appraisal Process

The appraisal of risk treatment will require RTAP to undergo the risk management process given in Figure 1, from Establishment of context till the Risk treatment, except that the cyclical portion will be undertaken by the applicant after successful evaluation of the application, as needed.

As a first step, RTAP will establish the context, followed by a detailed risk assessment. The risk assessment allows to determine the risks, improve their understanding and to allow RTAP to break the risks down into components. This helps evaluating and gauging the level of each of these component risks. Risk assessment includes the overall process of risk identification, risk analysis and risk evaluation (see Figure 1). After the risk assessment, the RMP will be reviewed by RTAP and analysed to understand the mitigation measures or controls being proposed and whether these controls adequately treat the risk to meet the objective (IEC/ISO 31010).

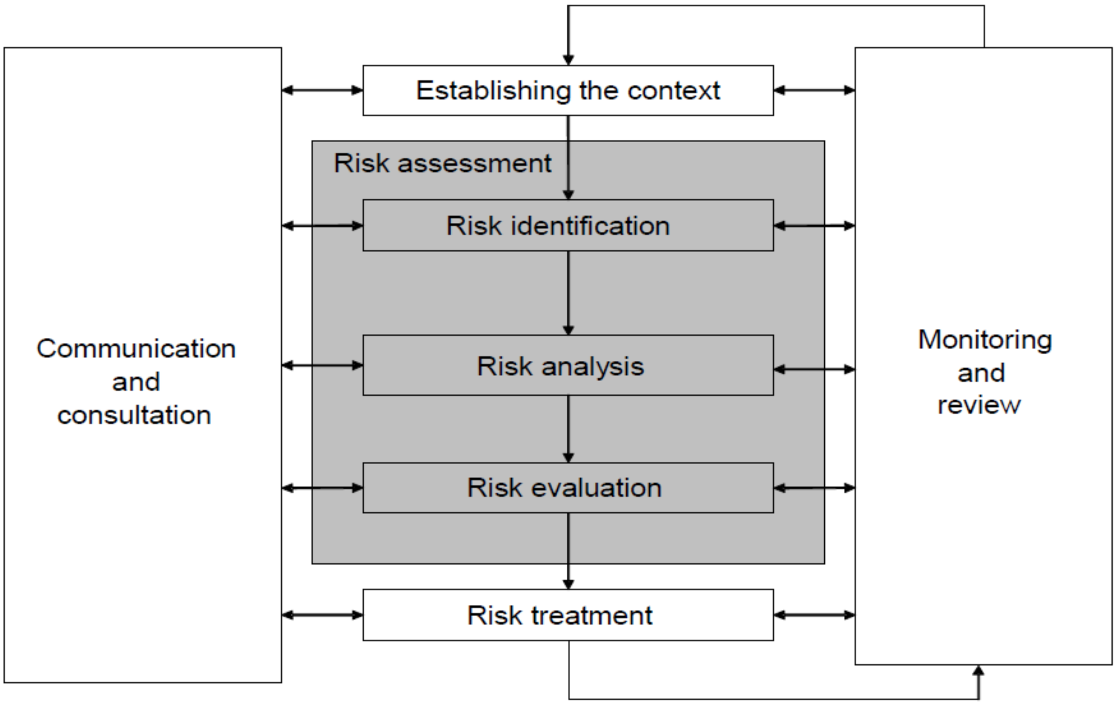


Figure 1: Risk Management Process (IEC/ISO 31010)

Risk assessment provides an understanding of risks, their causes, consequences and their probabilities, and provides input to decisions about the following (IEC/ISO 31010):

- whether an activity should be undertaken;
- choosing between options with different risks;
- prioritizing risk treatment options; and,
- the most appropriate selection of risk treatment strategies that will bring adverse risks to a tolerable level.

RTAP will first undertake **risk identification**, which is the process of finding, recognizing and recording risks, using one or more of the risk identification methods, like systematic team approaches and inductive reasoning approaches, e.g. HAZard and OPerability study (HAZOP) and Failure modes and effects analysis (FMEA) (IEC/ISO 31010). Then RTAP will conduct the **risk analysis** to determine their consequences (or severity) and probabilities (or likelihood), considering any existing controls and their effectiveness. Combining the consequences and their probabilities will determine the level of risk. Methods used in analyzing risks can be qualitative, semi-quantitative or quantitative. The degree of detail required will depend upon the application and the availability of reliable data. However, at least a semi-quantitative method will be used, using linear numerical rating scales for consequence and probability and combining them to produce risk level, with a clear explanation of all the terms employed and the basis for all criteria. Finally, RTAP will conduct **risk evaluation**, using the understanding of risk obtained during risk analysis phase to make decisions about future actions, including whether a risk needs treatment and its priority for treatment. The risks will be divided into at least three bands:

a. an upper band where the level of risk is intolerable whatever benefits the activity may bring, and risk treatment is essential whatever its cost;
b. a middle band (or 'grey' area) where costs and benefits, are taken into account and opportunities are balanced against potential consequences;
c. a lower band where the level of risk is regarded as negligible, or so small that no risk treatment measures are needed.

Risk treatment or mitigation involves selecting one or more options for modifying risks, and implementing those options. The risk treatment will be proposed by the applicant in RMP and it will be appraised for its effectiveness to meet the objective by RTAP. Risk treatment appraisal will require the RTAP to review and analyze the RMP. RTAP will breakdown the RMP into its constituent proposed controls and match these with the component risks evaluated. This will allow RTAP to gauge whether the RMP effectively treats the risks evaluated to adequately meet the objective. RTAP will communicate with ICANN organization and the applicant, as needed, to understand the objective and the RMP, while gauging the effectiveness of the treatment.

6 Risk Treatment Appraisal Panel (RTAP)

Effective risk analysis and mitigation would require a practitioner and expert in the area of risk management to help guide the discussion, coordinate the assessment work, and write the reports in collaboration with the other panel members. The team doing the risk analysis would also need experts who understand what are internationalized domain names and how are these implemented by the registries (to review the practicality of implementing the RMP), how IDNs may be confused, to what extent such confusion can cause harm and how such confusion and harm could be prevented.

Therefore, the RTAP will have members with the following roles. A member may address more than one role. RTAP panel will have three (3) to four (4) members, filling the following roles:

1. Expert for managing risk in technical projects, with experience in risk mitigation.
2. Expert on IDN implementation in registries, who understands the implementation opportunities and challenges for different IDN policies at the second and other levels.
3. Expert on the Unicode standard and security mechanisms related to the Unicode standard. Added expertise of designing IDN tables would be very useful.
4. Expert in brand protection in using domain names, with experience with current phishing practices, their impact and measures to address them.

7 Criteria for Risk Treatment

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

1. **Comprehensive:** The measures must specifically and explicitly address all the case(s) of confusing TLD labels, and all relevant aspects of confusion identified in each of the case(s) due to the applied-for TLD label.
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 for all identified aspects to an acceptable level.
3. **Conservative:** As the applied-for TLD label is already deemed confusable, any reasonable doubt on whether a mitigation measure can effectively address a certain aspect of the confusability should be resolved by erring on the side of considering it insufficient.
4. **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.

8 Risk Treatment Appraisal (RTA) Reports

There are two reports generated by the panel. There is *RTA-Interim Report* which identifies the gaps and (possibly) recommends any additional controls and solutions. The second *RTA-Final Report* provides the final consolidated recommendation after evaluating the RMP by the applicant. These reports would contain at least the following contents.

8.1 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 applicant, 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, 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?*

8.2 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 final RMP by the applicant, 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, evaluation if the residual risk is still at significant level? Why? Why not?*
8. *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?*

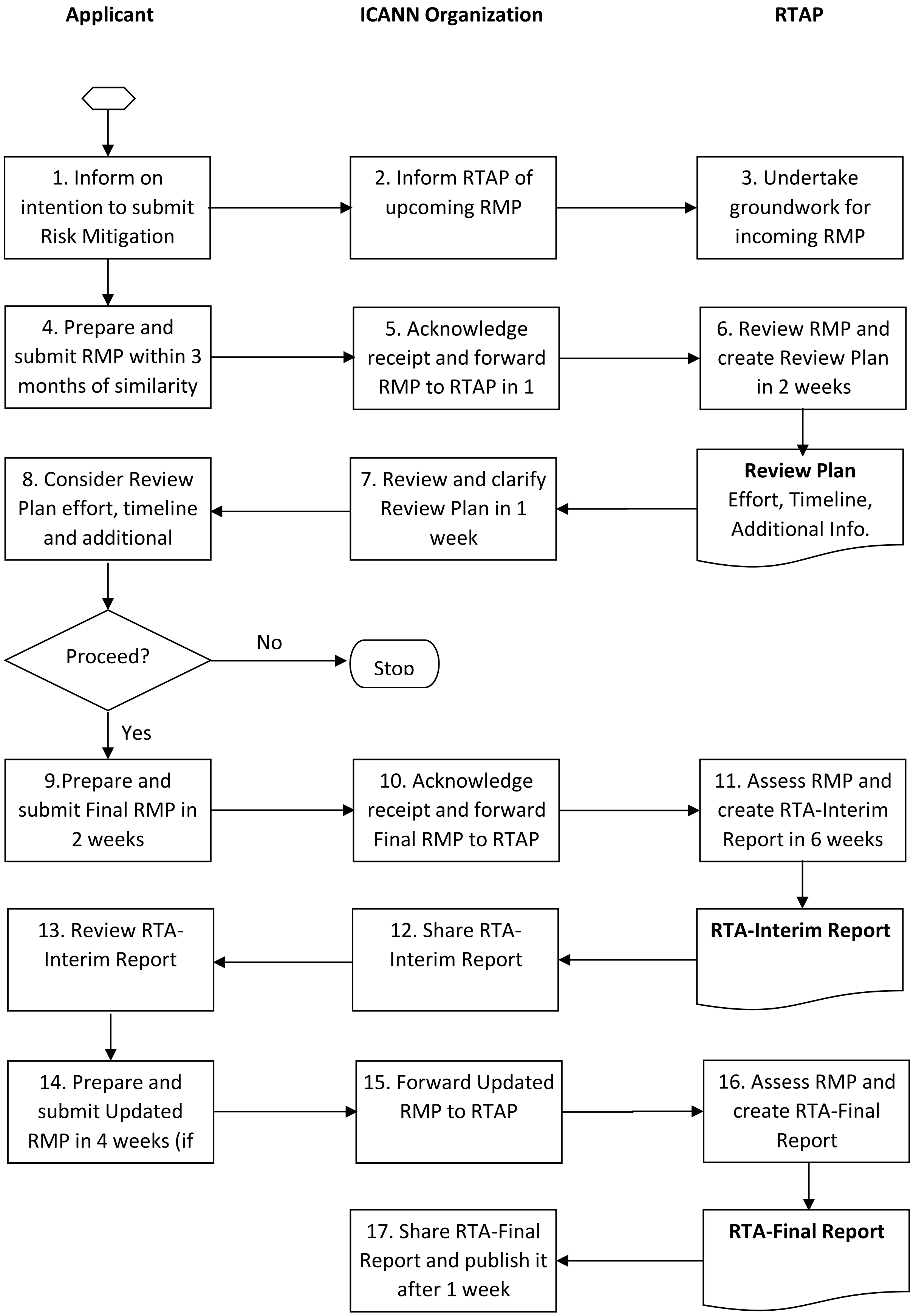
9 Application and Appraisal Procedure

1. Applicant informs ICANN organization its intention to submit RMP as soon as it decides to take this course, but no later than within three (3) months of the communication of the string similarity review decision
2. ICANN organization convenes RTAP to review the anticipated RMP
3. RTAP undertakes the ground work to prepare for the incoming RMP
4. Applicant provides a RMP within three (3) months of the communication of the string similarity review decision[2]
5. ICANN organization forwards RMP to RTAP within one (1) week of receiving it
6. RTAP creates a review plan within two (2) weeks for the completion of the work
   a. Estimated hours per panelist
   b. Tentative work plan and timeline
   c. Additional information which may be needed or helpful
7. ICANN organization appraises the review plan, asks any clarifying questions from RTAP within one (1) week, and informs the applicant on the cost and the timeline and any additional information needed
8. Applicant considers the review plan and confirms its intention to proceed
9. Applicant shares any feedback, any additional information requested, and confirms its intention on supporting the additional cost incurred within two (2) weeks. If the confirmation is not received in two (2) weeks, the application is closed

[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.

10. ICANN organization forwards Final RMP to RTAP
11. RTAP undertakes analysis of the RMP. ICANN organization coordinates any clarifying question between RTAP and the applicant (each question must be responded within a week by the applicant or else RTAP may move forward without the response). RTAP creates RTA-Interim Report and hands it over to ICANN organization within six (6) weeks of receiving the updated RMP
12. ICANN organization passes RTA-Interim Report to the applicant
13. Applicant reviews the RTA-Interim Report
14. Applicant submits response to RTA-Interim Report and an updated RMP (if any) to ICANN organization within four (4) weeks of receiving the RTA-Interim Report
15. ICANN organization sends the response from the applicant and updated RMP (if any) to RTAP. After four (4) weeks if the feedback is not received by the applicant, RTAP may continue to next steps
16. RTAP creates the RTA-Final Report and sends it to ICANN organization within (4) weeks of receiving the applicant response on RTA-Interim Report. ICANN organization coordinates any clarifying questions between RTAP and the applicant.
17. ICANN organization sends the RTA-Final Report to the applicant and publishes the RTA-Final Report after one (1) week of sending it to the applicant

9.1 Process Flow Diagram


Applicant
ICANN Organization
RTAP
1. Inform on intention to submit Risk Mitigation
2. Inform RTAP of upcoming RMP
3. Undertake groundwork for incoming RMP
4. Prepare and submit RMP within 3 months of similarity
5. Acknowledge receipt and forward RMP to RTAP in 1
6. Review RMP and create Review Plan in 2 weeks
Review Plan
Effort, Timeline, Additional Info.
7. Review and clarify Review Plan in 1 week
8. Consider Review Plan effort, timeline and additional
Proceed?
No
Stop
Yes
9.Prepare and submit Final RMP in 2 weeks
10. Acknowledge receipt and forward Final RMP to RTAP
11. Assess RMP and create RTA-Interim Report in 6 weeks
RTA-Interim Report
12. Share RTA-Interim Report
13. Review RTA-Interim Report
14. Prepare and submit Updated RMP in 4 weeks (if
15. Forward Updated RMP to RTAP
16. Assess RMP and create RTA-Final Report
RTA-Final Report
17. Share RTA-Final Report and publish it after 1 week