Work Track 5

Risk-Based Approach

What is a “Risk-based approach” in relation to policy development

- Risk management is a tool that helps organisations evaluate risks. Risk assessment is repeatable and objective; it allows you to replace an otherwise subjective “gut sense” with a more guided decision-making approach.

Identify Risks	Impact	Likelihood	Mitigation
What are we trying to prevent? and/or Who are we trying to protect?	Why are we trying to prevent the risk?	Based on what evidence?	How can we manage this risk effectively?
What	Why		How

Why use a “Risk-based approach” for WT5?

- Other approaches on this topic have not been effective
- The risk-based approach is concerned with identifying, understanding and mitigating risks rather than to resolve entrenched positions of SO/ACs within ICANN
- The output can effectively be inserted into policy (what & why) and implementation (how).
- It is versatile for future (monitor results, re-assess and adapt)

How do we apply a “Risk-based approach” for WT5?

1. Identify risks (within the scope of WT5)

2. Assess risks (impact/severity, likelihood, what is acceptable, what is not acceptable)

3. Address the risks (how can we avoid/eliminate or mitigate the risk?)

4. Monitor effectiveness / continual improvement

Risk Register

The risk register records identified risks, their severity, probability of occurrence, and the actions steps to be taken.

Risk description	Potential causes	Harm/consequences	Impact (1-5)	Likelihood (1-5)	Risk Score (Impact x Likelihood)	Controls
What is the risk we are concerned about?	How could these risks be triggered?	What could be the consequences?	An assessment of the impact that the occurrence of this risk would have. (1=negligible, 5=catastophic)	An assessment on how likely it is that this risk will occur. (1=improbable, 5=frequent)	Helps prioritise efforts.	Policy/controls to prevent or mitigate the risk.

The advantage of creating a risk register is that this can regularly be reviewed to assess effectiveness of controls based on evidence (backwards looking) and also for their robustness towards new and emerging issues (forward looking). This can then inform policy makers of potential changes needed to ensure the controls continue to meet their intended purpose.

Addressing the risks

The suite of existing controls can be leveraged when we come to address the identified risks. These controls may be effective in isolation or as a combination of controls throughout the different stages (pre-application, application, post-delegation).

Pre-application	Application	Post-delegation
Block/not permitted Restricted (Pre-application conditions to limit who can apply, e.g. permission/no objection letters)	Objections and GAC advice (Application control to allow for community assessment) String similarity checks (Application control to prevent confusion) PICs (Application control to apply additional terms for use)	gTLD Registry Agreement Monitoring - operational compliance Dispute mechanisms e.g. PICDRP

Task 1

Identify Risks	Impact	Likelihood	Mitigation
What are we trying to prevent? What are we trying to prevent? and/or Who are we trying to protect?	Why are we trying to prevent the risk?	Based on what evidence?	How can we manage this risk effectively?
What	Why		How