ICANN Enterprise Risk Management Process

Introduction:

ICANN has a proven commitment to accountability and transparency in all of its practices. Indeed, ICANN considers these principles to be fundamental safeguards in ensuring that its international, bottom-up, multistakeholder model remains effective. This summary is intended to provide a brief insight into ICANN's risk management activities.

Over the course of ICANN's history, we have leveraged many mechanisms and experts to assist with identifying the risks posing threats to ICANN. Specifically, ICANN has worked with a variety of experts over the years to conduct internal enterprise-wide, new gTLD, and DNS risk assessments, among others. In 2013, ICANN formally established a specific department to oversee enterprise risk management (ERM). The ERM department is tasked with helping identify risks that, if they occurred, could affect the organization, as well as tracking mitigation plans and implementation, and reporting on the results of those efforts.

Since late 2008, ICANN's Board Risk Committee has been in place to oversee the processes and methodologies noted above. Specifically, the Board helps ensure that management has properly gauged the risk appetite and risk profile for ICANN, and that a sound mechanism is in place to address and mitigate, as applicable, the identified risks.

Definition of Risk:

According to many, the definition of risk is as simple as the possibility of something bad or unanticipated occurring that results in loss or harm. This is important to note, as ICANN has taken integral steps in the identification, evaluation and mitigation of risks that could potentially and adversely affect ICANN's mission.

The Process:

How does ICANN identify, evaluate and mitigate risk?

ICANN relies on a sound and commonly used risk management model and in consultation with risk and subject matter experts to:

1) Identify risks via surveys, inquiries, community feedback, working groups, etc.
2) Evaluate the level of impact to the organization, as well as the probability that each risk will occur.
3) Assess the risk and make the necessary determination regarding level of mitigation efforts. Examples include:
    - Accepting the risk and monitor it's impact level

- Avoiding the risk by eliminating or altering the circumstances causing the risk
- Reducing/mitigating the risk and its impact by putting proper controls in place.
- Sharing responsibility for risk mitigation with other parties, in order to minimize the risk impact, such as purchasing insurance to cover potential financial losses associated with a risk.

To explain the process and an example of one such risk assessment conducted by ICANN, you can find the details at the link below:
https://www.icann.org/news/announcement-2014-05-28-en

ICANN Enterprise-Wide Risks:
ICANN has identified the following enterprise-wide risks via the processes mentioned above. It is anticipated that the list below will evolve over time, as other risks may be identified and/or created as a result of various activities, such as new policy implementation, new projects or programs undertaken, etc. Below is a list of enterprise-wide risks that ICANN is currently managing. Note that this list is in no particular order.

- Failure to adequately maintain and adhere to existing accountability mechanisms.
- Failure to demonstrate sufficient accountability and transparency of organization
- Lower revenues than forecasted.
- Adverse legal or other dispute resolution ruling, including possible related penalties, fees and costs.
- Failure to sufficiently manage and enforce the hundreds of contracts with TLD operators.
- Unsuccessful delivery of a stakeholder proposal and other relevant deliverables for a successful NTIA stewardship transition of the IANA Functions.
- Significant financial loss, other than lower-than-anticipated revenues (e.g., fraud, investment loss, etc.).
- Potential issues for New gTLD Program related to accountability mechanisms due to possible adverse decision or failure of mechanism/process.
- Unfunded operational costs or unplanned expenses.
- Potential perception that not all conflicts of interests are identified during decision-making process.
- Possible perception that ICANN has poor global engagement, transparency, policy, coordination and communication.
- Significant increase in legal or other dispute resolution filings that could challenge staff capacity, distract leadership and disrupt operations.
- Policy development process is too slow or ineffective, participants decrease or stagnate, or failure to bring new stakeholders into the model.
- Potential legal actions from parties that believe that they have been injured resulting from New gTLD Program.

- Significant revenue reduction (e.g., reduced domain name volume, reduced ccTLD contributions, reduced registrar fees, etc.).
- Perception of failure to implement and help achieve a global multi-stakeholder distributed IG ecosystem according to the widely accepted Net Mundial Principles.
- Possibility that current supporting organization and advisory committee (SO/AC) structures cannot scale to include and support new global entrants and participants.
- Unsuccessful implementation of adopted recommendation resulting from various Affirmation of Commitment reviews.
- Insufficient progress towards major project implementation (e.g., gTLD, IDN fast track, DNSSEC, etc.).
- Inability to deliver commitments (mission, operational objectives, strategic initiatives) due to limited resources, budget, or prioritization.
- Key skills depart ICANN (consultants or staff) without clear succession plan for continuation of operating functions or exchange of knowledge and documentation.
- Lack of improving trust in the multi-stakeholder model.
- Contracted party non-payment or service provider non-performance (e.g., registrar, registry, and vendors).
- Failure to effectively facilitate international participation in DNS Technical Coordination in the event of significant Internet security, stability or resiliency incident.
- DNS vulnerability to attacks (root) causing disruption to Internet operability (DDoS Attacks, Cache Poisoning, etc.).
- Potential data breach of personal or confidential data from ICANN systems; confidential data made public.
- Failure of the community accountability process to adequately address ICANN accountability in light of its changing historical relationship with the USG.
- Ineffective contractual compliance approach, process, and audits (registries, registrars, others).
- Inconsistent communication and messaging to stakeholders, leading to confusion and lack of understanding.
- Poor fiscal policy-making or gross mis-management.
- Potential for ineffective technical business continuity management given an event occurs (e.g., data back-up, disaster recover planning, data outage, etc.).
- Potential lack of operational efficiency, excellence and discipline due to lack of internal collaboration and clearly defined roles and responsibilities.
- One or more governments' policy changes that negatively affect different sectors of a stakeholder or regional work and current functionality of SO/AC model.

To find details of strategic risks that ICANN may face, please click the link below to the 'ICANN Strategic Plan for fiscal years 2016-2020'.

https://www.icann.org/en/system/files/files/strategic-plan-2016-2020-10oct14-en.pdf

How the Identified Risks Are Addressed:
Once identified, the risk is rated based on the likelihood that the risk will occur, as well as the level of impact to the organization. This is performed via leveraging a consistent rating scale and gauging where the risk sits on that scale. Once the risk is rated, a decision is made whether mitigation or remediation of the risk is necessary. If necessary, the assessment of the decision to undertake mitigation will result in the remedies that are needed to reduce the risk impact and likelihood to the organization.

As normal operating procedure for ICANN, we will continue to annually identify and evaluate new and existing risks, whether actual, potential or perceived, and ensure that proper risk mitigation and remediation efforts are in place on a going forward basis.

It's important to note that specific details and decisions taken to address many of the risks above are considered confidential and will not be disclosed. Maintaining confidentiality of risk mitigation efforts until they are fully operational and public, if appropriate, is a standard risk management practice: by disclosing decisions and courses of action planned or taken to address specific ICANN related risks, ICANN could introduce an entirely new set of risks caused by such disclosure.