ICANN 72

VIRTUAL ANNUAL GENERAL

**Overview of ICANN Org
Risk Management Framework**

Meeting Agenda

Introductory remarks from Xavier Calvez SVP, Planning & Chief Financial Officer

Overview of ICANN Org Risk Management Framework
1 Document Scope
2 Risk and Risk Management Defined
3 Background and Development of Risk Management Framework
4 Risk Strategy and Appetite
5 Risk Governance and Accountability
6 Risk Culture
7 Risk Assessment, Controls, and Reporting

Concluding remarks from Lito Ibarra, ICANN Board Risk Committee Chair

Questions

1 Document Scope

This Overview of Risk Management at ICANN organization (org) is meant to provide a briefing on ICANN's risk management activities. It covers the risk management framework and how it is implemented and operationalized. This overview does not cover specific risks faced by ICANN nor the corresponding countermeasures.

These presentation slides are a summary of the Overview of ICANN Org Risk Management Framework document. For more detail, please refer to the document available on icann.org:

https://www.icann.org/en/system/files/files/icann-org-risk-management-framework-overview-29sep21-en.pdf

Risk and Risk Management Defined

Risk is the possibility of events, conditions, or trends to have an adverse impact on ICANN's ability to achieve its mission and strategic plan and could even prevent ICANN org from continuing its operations. Importantly, risk is characterized by some element of uncertainty.

Managing risk entails evaluating that portfolio of risks and managing them. Risk management is not the elimination of all risks.

The Board and Executive Team are responsible for knowing what risks ICANN faces and making informed decisions to set the accepted level of risk, in other words the risk appetite.

The goal is for there to be no surprises. To that end, Risk Management is important for the planning processes with two-way inputs between risk management and the planning processes.

Development of Risk Management Framework

In 2014-2015, ICANN refreshed to the org's Risk Management Framework. The org and the Board Risk Committee, with the assistance of an external consulting firm, developed a Risk Management Target Model that was supported by the Board and is the basis of the org's current Risk Management Framework.

The Target Model is based on the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Enterprise Risk Management Integrated Framework and selected the desired level of maturity (development) for various elements of the Risk Management Framework.

The org has achieved, and in some cases exceeded, the target maturity levels. Progress is reported regularly to the Board Risk Committee and annually to the full Board.

	Weak	Sustainable	Mature	Integrated	Advanced
Risk Strategy & Appetite			• Risk considered • Risk strategy is defined • Risk appetite is defined	• Risk integrated organization-wide • Board sets risk direction • Board has clear view & direction of risk	• Risk integrated • Risk strategy Dev • Risk appetite is reflective of advance measurement tech
Risk Governance			• Risk Management function exist • Risk considered consistently across all organization	• Risk embedded within operating model • Standards & policies defined centrally	• Risk integrated into activities • Organization-wide risk guidance & approach
Risk Culture		• Risk culture is driven by few unifying big-pictures themes • Formal risk comm occurs in silos	• Risk consistent tone from top level • Risk management performance is measured	• Risk ownership, transparency, & forward-looking views • Performance targets are risk adjusted	
Risk Assessment & Measurement		• Risk assessment & measurement process exists, but not formal • Risk quantification defined	• Organization-wide approach to risk ID and applied consistently • Clarity on risk measurement method	• Risk ownership, transparency, & forward-looking views • Performance targets are risk adjusted	
Risk Management & Monitoring		• Limited assurance process to test and validate risk mitigating activities	• Established assurance process to test and validate risk mitigating activities	• Integrated process to test and validate risk mitigating activities	
Risk Reporting & Insights		• Board & Senior management received regular reports on risk positions & effectiveness	• External communication on risk are well defined and proactively managed	• External communication on risks is both well defined and adaptive	
Data & Technology		• Data governance is broadly defined • Defined roles & report exists to monitor data quality & integrity	• Qualitative & quantitative risk analytics & enabling systems/tools are defined and implemented	Key qualitative & quantitative risk analytics & enabling systems/tools are defined & functionality is implemented	

Target reached ▭   Target exceeded ▭

ICANN

4 Risk Strategy and Appetite

The Risk Appetite Statement articulates the level of risk that ICANN organization is willing to take and retain on a broad level to fulfill its mission. The Board approved ICANN org's first Risk Appetite Statement in December 2020.

"ICANN's overall risk appetite is low to medium. As a nonprofit, public benefit, mission-driven organization supporting the security, stability, and resiliency of the Internet, ICANN operates within a low risk appetite for risks directly related to its critical mission. ICANN has a low or medium risk appetite for risks related to operating the ICANN organization as it balances its operations with the resources required to manage the associated risks."

https://www.icann.org/en/blogs/details/icann-board-approves-the-risk-appetite-statement-22-12-2020-en

5 Risk Governance and Accountability

VP of Risk Management who reports to SVP, Planning and Chief Financial Officer (CFO) and who works with personnel, org executives, and the Board to implement and operationalize the Risk Management Framework.

Key to the risk management approach at ICANN org is the ownership of risks, thereby establishing accountability of specific risks.

There is formal governance oversight of the Risk Management Framework and Risk Management. The Risk Management Policy describes the role and responsibility of various risk management participants.
* Board of Directors and Board Risk Committee
* President and CEO
* CEO Risk Management Committee
* Risk Liaisons
* Risk Management Function
* All ICANN Personnel

An important goal of an effective Risk Management Framework is that it must be understood and applied by personnel in an organization. ICANN org strives for all personnel to understand and apply the Framework.

ICANN's goal is to promote a risk-aware culture, where everyone is a risk manager.

Risk Assessment, Controls, and Reporting

The Risk Assessment, Controls, and Reporting elements of the Risk Management Framework are part of the same cycle of Risk Management activity that culminates in the org's Risk Register as managed under the org's Risk Identification and Management Procedure.

DRAFT

Risk Assessment, Controls, and Reporting

Identifying Risks

- Annual refresh of risks.
- Quarterly validation.
- As risks are identified.
- Risks identified as part of other ICANN org and community processes are also considered.

Risk Measurement and Org Risk Register

- Identified risks are rated for likelihood, impact, and control effectiveness.
- Controls and mitigations described.
- If appropriate, action plans for additional controls and mitigations.
- Ratings calibrated to ensure consistency across risks and materiality thresholds.

Risk Controls

- Controls and mitigations are reviewed quarterly as part of the quarterly validation.
- Included in the Risk Register reviews and oversight.
- The Risk Management function has begun a periodic evaluation of controls.

Monitor
Annual Risk Register refresh and quarterly validations. Risks are reevaluated and progress of risk-reducing actions plans are updated. Risk Management evaluates the controls and mitigations.

Reporting
Periodic reporting on the ICANN org Risk Register
- CEO Risk Management Committee: Top Risks three to four times per year, full ICANN org Risk Register annually.
- Board Risk Committee: Top Risks three to four times per year, full ICANN org Risk Register annually.
- Full Board: Top Risks two times per year, full ICANN org Risk Register annually.

Periodic reporting on existential risk(s) to ICANN org. These risks may include risks that have such a low probability that they would not be included in the Risk Register, but this process captures such risks for consideration.

Risk reporting shared as needed within the org for planning and other purposes.

Questions

Questions and Answers