Overview of ICANN Org Risk Management Framework

ICANN Organization

Risk Management
October 2022

TABLE OF CONTENTS

1 Document Scope

This "Overview of ICANN Org Risk Management" (Overview) is a briefing on ICANN organization's (org's) risk management activities. It covers the org's risk management framework and how it is implemented and operationalized. This Overview does not cover specific risks faced by ICANN nor the corresponding countermeasures. Risks often involve vulnerabilities or threats to ICANN, and it would be imprudent for the org to provide details of such risks. Additionally, risks faced by ICANN can include legal implications that should not be disclosed outside of the org or the Board.

This document is an update to the September 2021 Overview. In addition to some minor edits for clarity, this update reflects that the annual risk controls assurance process that was previously being implemented, is now operational.

2 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.

A Risk Management Framework: (i) creates a holistic, portfolio view of the most significant risks to the organization's mission; (ii) unifies the various risk management activities across the organization for a comprehensive approach and identifies risk management gaps; and (iii) provides assurance to Executive Management and the Board that the organization is operating safely in support of ICANN's mission.

Managing risk entails evaluating that portfolio of risks and choosing which risks to accept, to reduce, and to avoid. ICANN org promotes efficiency by managing risks to its mission, not necessarily eliminating all risks. Eliminating all risks would paralyze any organization when attempting to mitigate all potential negative events regardless of how unlikely or how immaterial.

The Board and Executive Team are responsible for knowing what risks ICANN faces, how those risks are being managed, and what residual risks remain by keeping the risk register updated, including identification, likeliness, severity, and mitigation of risks. The Board and Executive Team also are responsible for using that information to make an informed decision to set the accepted level of risk, in other words the risk appetite. In order to inform the Board and Executives, the organization must articulate ICANN's risks and risk management controls, and plan for any additional controls.

Adverse events will occur; however, the org wants to anticipate and manage risks, not be reactive. 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.

3 Background and Development of Risk Management Framework

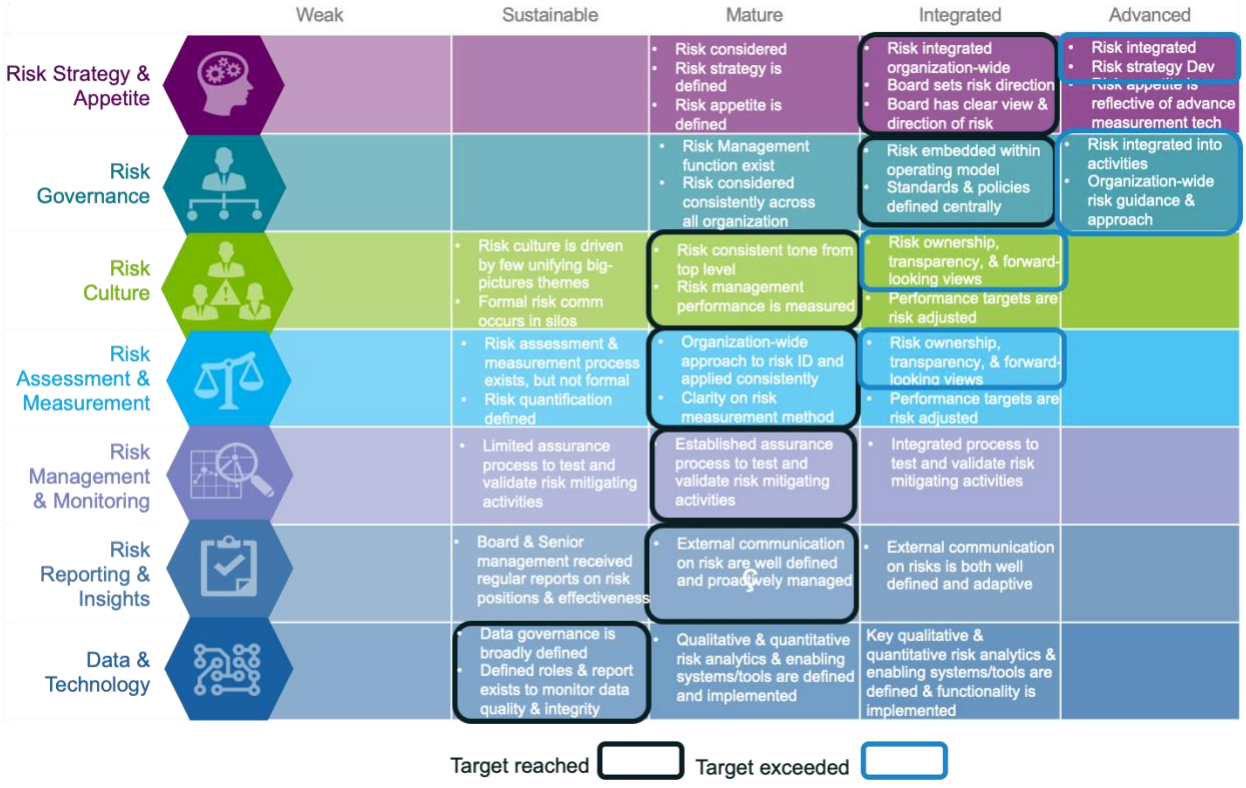
In 2014-2015, ICANN initiated an update to the org's Risk Management Framework. The org and the Board Risk Committee, with the assistance of an external consulting firm, developed a Risk Management Target Model that was supported by the Board and is the basis of the org's current Risk Management Framework.

The Target Model is based on the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Enterprise Risk Management Integrated Framework that is a widely used framework by organizations and considered a leading practice. The Target Model selected the desired level of maturity (development) for various elements of the Risk Management Framework such as risk appetite and governance model, among others. The desired maturity of the elements is based on cost/benefit, relative complexity of the org, and other factors.

The org has achieved, and in some cases exceeded, the target maturity levels. The target maturity of each element is represented in the chart below with black rings, all of which have been achieved. The blue rings represent where the maturity target level has been exceeded. The maturity of the most important elements of the Target Model has been exceeded due to the natural evolution of the risk management program at ICANN org.

Risk Management Target Model - Maturity Matrix

Summary Objectives by Maturity Level



In early 2021, the org reviewed the Risk Management Target Model and determined that the current levels of maturity, including exceeding the original targets, continue to be appropriate. The Target Model was shared with and reviewed by the Board Risk Committee and the Board.

Risk Management Target Model - Detailed

Detailed Objectives for Each Element at Target Maturity

	MATURITY LEVEL	TARGET	OBJECTIVE(S)	KEY SUCCESS FACTOR
Risk Strategy & Appetite	Advanced / Integrated	• Risk integrated organization-wide • Board sets risk appetite.	-Risk policy/appetite updated annually -Risk management is linked with strategic and operating planning and other sources of risk identification	Risk appetite approved by Board annually
Risk Governance & Accountability	Advanced / Integrated	• Risk integrated into activities • Organization-wide risk guidance & approach	-Defined roles and responsibilities for risk management -Effectiveness of Risk Management is assessed	Oversight by the BRC and the CEO Risk Management Committee of risk management activities
Risk Culture	Integrated / Mature	• Risk tone consistent from top level • Risk management performance is measured	-Risk Appetite Statement is understood and applied in the org and Board -All staff are risk managers	Risk aware culture is evident throughout the org and Board
Risk Assessment & Measurement	Integrated / Mature	• Consistent Organization-wide approach to risk ID • Clarity on risk measurement method	-Risk Register is understood by CEO Risk Management Committee and BRC; presented to the Board. -Risk ratings drive goal-level RM metric	Assessment and measurement process is understood and stable
Control Effectiveness	Mature	Established assurance process to test and validate risk mitigating activities	-Risk mitigating activities are documented and monitored -Effectiveness of risk mitigating activities is evaluated and reported	Regular reporting of control effectiveness
Risk Reporting & Insights	Mature	Reporting and communication on risk is well defined and proactively managed	-Regular useful reporting to or executives, the BRC, and Board. -External communications of Risk Management Framework	Staff accountability and responsibility of RM exist at an executive level
Risk Management Technology	Sustainable	End User Computing is used to gather and catalogue risk information.	Risk information captured and analyzed is defined and reviewed Adequate tool supports the defined nature and volume of the data	Stable and accurate records. Useful reporting.

4 Risk Strategy and Appetite

Risk Appetite Statement

The Risk Appetite Statement (Statement) articulates the level of risk that ICANN org is willing to take and retain on a broad level to fulfill ICANN's mission. Which risks and the level of risk ICANN faces must be understood to develop the Statement. Therefore, the Statement was the last major element of the Risk Management Framework to be completed. The Board approved ICANN org's first Risk Appetite Statement in December 2020 and directed the publication of a Summary Risk Appetite Statement document. The Statement, updated as appropriate, will be presented to the Board annually.

ICANN org's overarching Risk Appetite Statement is:

"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."

A Risk Appetite Statement:

- Communicates to personnel that they must pursue objectives within accepted risk limits.
- Provides input for prioritization for planning and budgeting.
- Guides the Board in its decision-making and can be considered as part of the rationale that accompanies Board resolutions.
- Guides personnel to make decisions that are aligned with the organizational risk appetite.
- Encourages a risk management, not risk aversion, culture so that risk management is a responsibility shared across the organization and for which all personnel are accountable.
- Enhances ICANN's reputation by demonstrating that the organization is committed to proactively managing risk.

Risk Management Policy

ICANN organization's Risk Management Policy (Policy) is an internal document that communicates the guiding principles and requirements of risk management at ICANN org, including related procedures.

The Policy advances the following:

- Active identification and articulation of risks, providing for informed decisions regarding the level of risk being taken, and allowing for a deliberate decision to be taken regarding risks.
- Transparency of risks so that risks are managed before they become a threat to fulfilling the organization’s objectives. The goal is to ensure that there are no surprises.
- A risk-aware culture, where all personnel feel empowered to identify and escalate risk concerns. Staff and functions own the risks from their activities and the required responses.
- Operational efficiency from effective risk controls that reduce disruption to organizational objectives.
- Concise and insightful reporting to the Executive Team and the Board.

The requirements of the Policy are:

- An accountability structure between the Board and org. Please see the section on Risk Governance and Accountability.
- A Risk Identification and Management Procedure. Please see the section on Risk Assessment.
- A New Activity Procedure that requires significant new activity to be assessed for material risks.
- A Continuity Planning Procedure to unify the org's continuity efforts to be integrated with crisis management and disaster recovery.
- Reporting to ensure all proper parties are informed as appropriate.
- Training to ensure that personnel are informed about risk management.

5 Risk Governance and Accountability

Structure of Risk Management in ICANN Org

The Risk Management function of ICANN org consists of a vice president who reports to the 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. The ICANN President and CEO owns all risks within the org and delegates functional ownership of each identified risk to the most relevant org executive. This accountability model means that the Risk Management function is not the owner of risks, but the facilitator of the Risk Management Framework within the org.

The Risk Management function is supported by a Risk Liaison from each function. Each function executive appoints a member of their team to serve as a Risk Liaison. This leverages the expertise within the function for risk management purposes and provides each function with a risk management contact. This staffing model is consistent with ownership of risks by the function closest to the activity giving rise to a particular risk, and has several advantages compared to building a large risk management staff.

To ensure that the objectives of the Risk Management Framework are being fulfilled, there is formal governance oversight of the Risk Management Framework and Risk Management activities as described in the Risk Management Policy.

Within the org, there is a CEO Risk Management Committee made up of several org executives, including the President and CEO, that meets regularly to provide oversight to ensure that the Risk Management Framework is operating effectively. The Board Risk Committee has oversight of the Risk Management Framework and the org's risk management activities. The Board Risk Committee reports to the Board semi-annually on the status of the Risk Management Framework, material risks identified by the org, and other risk management initiatives.

Roles and Responsibilities

	Role and Responsibility
Board of Directors and Board Risk Committee	Ultimately responsible for ICANN and the types and amount of risk that the organization will accept (as expressed in the Risk Appetite Statement). Oversee that the organization operates within the articulated appetite through reporting that that the Risk Management Framework is being followed.
President and CEO	Responsible for Risk Management within ICANN organization. Sets the tone from the top for the success of Risk Management. Approves or rejects recommendations of the CEO Risk Management Committee and Risk Management function.

CEO Risk Management Committee	Made up of ICANN org executives, including the President and CEO, provides oversight of the Risk Management activities of ICANN org. Provides expertise and feedback in the design and implementation of the Risk Management Framework and advises the President and CEO on risk-related matters. Reviews risk reporting and requires action as necessary. Reviews and recommends remediation and action plans, and ensures accountability for delivering such plans, as well as arranging the necessary resources to deliver the Risk Management Framework. Members are informed about risk management issues, and members become supporters of risk management and a risk aware culture, and sustain the risk management journey.
Risk Liaisons	Each function designates a liaison to the Risk Liaison Network who becomes the functional subject matter expert on risk management and is a resource for their function. Risk Liaisons facilitate risk management programs within their functions. Risk Liaisons report to their own function, which reinforces the ownership of risks at the function level.
Risk Management Function	Provides leadership and expertise for the implementation and operation of the Risk Management Framework. Develops procedures and tools to support the Risk Management Policy. Provides the appropriate level of facilitation and moderation to enable the organization to carry out the Risk Management Framework. Develops concise and insightful risk management reporting for management and the Board, or ensures that other functions of ICANN are fulfilling this responsibility. Working with the functions to identify and help manage its risks and operate within the defined risk appetite and identified risk mitigations.
All ICANN Personnel	Support the Risk Management Framework by executing relevant procedures and processes. Own the risks inherent in their activities and adopt the approach of “we are all risk managers.” Are empowered to escalate concerns.

6 Risk Culture

An important goal of an effective Risk Management Framework is that it must be understood and applied by personnel in an organization. While some organizations require only certain personnel to be aware of its Risk Management Framework, ICANN org strives for all personnel to understand and apply the Framework. There is a strong understanding of Risk Management by the Board, org Executive Team, and Risk Liaisons, as well as awareness among all ICANN personnel. ICANN's goal is to promote a risk-aware culture, where everyone is a risk manager.

7 Risk Assessment, Controls, and Reporting

Risk Identification Management

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

The org's Risk Identification and Management Procedure provides for:

- Active identification and articulation of risks to the organization, providing for informed decisions regarding the level of risk being taken by the organization and allowing for a considered decision regarding how to manage identified risks.
- Incorporating material risks identified in other org and community risk-identification activities.
- Inputs into org planning processes.
- Transparency of risks so that risks are managed before they become threats to fulfilling organizational objectives.
- Operational efficiency from effective risk controls that reduce disruption to organizational objectives.
- Data that informs the org's Risk Appetite Statement.
- Useful reporting to the Executive Team and the Board.

Risk Identification and Management is an iterative process that frequently refreshes and considers the risks facing functions and the organization, re-evaluates the organization’s appetite for the risks, and determines whether controls are appropriate and effective based on monitoring, and provides reporting to the Executive Team and the Board.

Identifying Risks

Annually, each ICANN org function conducts "annual refresh" of the Risk Register, to identify the risks the function faces, and to determine whether any rise to the org risk level. The risk-identification process is facilitated by that function's Risk Liaison with assistance from the Risk Management function and the risks are logged in a function-level Risk Register maintained by the Risk Liaison for that function. There are also annual risk control assurance sessions with each function, as well as an interim validation, where all functions review the risks the function owns that are in the org Risk Register.

Annual Refresh	July
Annual Risk Controls Assurance	November (post AGM)
Interim Validation	March

Org personnel are also encouraged to identify risks as they arise and follow the same processes; there is no reason to wait for the annual or quarterly process if a new risk is identified.

In addition to the work of the Risk Liaison Network, risks identified as part of other processes in the org and community are also considered for inclusion in the org Risk Register. If such a risk is identified, a risk owner within ICANN org is assigned and the standard process is applied. Other processes include Strategic Planning risks, the annual Trends Analysis performed by the Planning function, and issues raised by Board committees and community Supporting Organizations (SOs) and Advisory Committees (ACs).

Risk Measurement and Org Risk Register

Using a set of common definitions as a guide, each ICANN org function estimates the likelihood and severity for each risk, as well as the effectiveness of any existing controls or mitigation. Most of the risks faced by ICANN are subjective and require professional judgment for these estimates.

The function will recommend the risk decision for the risk (accept, reduce, or avoid, i.e., eliminate to the greatest extent feasible) and provide an action plan for cases other than accepting a risk. If additional mitigations are identified, the action plan should include specific time frames if feasible, as well as resources and budget requirements to implement the additional mitigation.

The Risk Management function and the Risk Liaison Network hold sessions to calibrate the identified risks across the organization, through discussion and comparison, to ensure that risks are consistently rated across the organization. They then determine which risks are sufficiently material to the org to be included in the org Risk Register. The CEO Risk Management Committee reviews the proposed register and ICANN's President and CEO approves the org-level Risk Register.

The Top Risks in the org Risk Register are reviewed regularly (three to four times per year) by the Board Risk Committee and updated to the full Board semi-annually. The complete org Risk Register is presented to the Board Risk Committee and full Board annually.

Risk Controls

As risks are identified and included in the org Risk Register, the risk owner identifies controls and mitigations, both those that exist now and action plans for any new controls and mitigations, if applicable.

The Risk Management function conducts annual risk control assurance sessions to review the controls in place in order to have a thorough understanding of the controls' effectiveness. Action plans for additional controls and mitigations are integrated with operational planning as appropriate. These sessions are also used to thoroughly review the risks owned by each of the functions with the respective function executive, Risk Liaison, and other subject-matter experts.

Risk Management provides reporting regarding the evaluation of control and mitigation effectiveness to the CEO Risk Management team and the Board Risk Committee.

Monitor

As described, the primary monitoring of the risks as part of the Risk Management Framework is the annual Risk Register refresh and quarterly validations. Risks are reevaluated and progress of risk-reducing actions plans are updated. Each risk owner is responsible for managing their owned risks as appropriate as part of normal operations.

Reporting

Periodic risk reporting is provided to the CEO Risk Management Committee and the Board Risk Committee. In particular, the reporting presents the top risks, changes in relative risk rankings, risk trends and changes, and actions to manage the risks. Status of risk mitigation action plans are also reported to the CEO Risk Management Committee. The reporting also may include further discussion of risks of particular interest or concern to the org, Board Risk Committee, or Board. The Board Risk Committee reports to the full Board on a semi-annual basis.

The above-referenced reporting also includes an annual report to the Board Risk Committee regarding existential risks to ICANN org. These risks may include risks that have such a low probability that they would not be included in the org Risk Register, but this process captures such risks for consideration.

In addition, the Risk Management function outputs its work to the org planning function so that the risks identified and managed as part of the Risk Management Framework can be considered, as appropriate, in planning activities.

Finally, this document is part of the fulfilling the goal of externally communicating about the org's Risk Management Framework.