Risk and Cybersecurity Committee Update

Rob Seastrom
ARIN Board of Trustees
Committee Chair

Overview

- What and Why
- Examples
- By the Numbers (Trends)
- What we use the Risk Register for
- Conclusions

What is the Risk Register? Why do we do this?

- Formal list of areas of concern
- Scoring of risk (*likelihood x impact = risk*)
  - Drives discussion of prioritization
- Remediation Plans (what we are doing to reduce risk to acceptable levels)
- Important because there is more to consider than we can hold in our minds at once.

Example Risk

Risk:

Risk of depleting ARIN’s reserves if our long-term revenue outlook does not cover anticipated expenses.

Remediation Plan Summary:

Revise ARIN's approach to investment reserve proceeds to align operating income with expenses. Move legacy clients to the same fee schedule as the rest of the Community. Develop a product strategy that aligns revenue & expenses with growth.

Impact Level (with current remediations): 1

Likelihood Level (with current remediations): 2

(another) Example Risk

Risk:

Introduction of malicious code, to include malware and ransomware

Remediation Plan Summary:

Enhance security awareness training program, automated reporting for all staff, review/enhance vulnerability management

Impact Level (with current remediations): 3

Likelihood Level (with current remediations): 2

By the numbers

While we are careful about talking about individual risks, we are happy to talk about aggregate numbers!

We are tracking:

28 top level risks in 2025q2, compared to

24 top level risks in 2024q2

Each risk is characterized as having a primary and secondary category between “strategic”, “operational”, “financial”, and “technical”.

By the numbers – total risks tracked

2025q2 (now)

- Strategic (13 primary 4 secondary)
- Operational (8 primary 4 secondary)
- Financial (2 primary 13 secondary)
- Technical (4 primary 1 secondary)

2024q2

- Strategic (9 primary 4 secondary)
- Operational (8 primary 3 secondary)
- Financial (2 primary 9 secondary)
- Technical (4 primary 1 secondary)

By the numbers – probability

2025q2 (now)

- Rising (3)
- Steady (15)
- Falling (10)

2024q2

- Rising (4)
- Steady (11)
- Falling (9)

Now that we've got it, what do we do with the Risk Register?

The Risk and Cybersecurity Committee:

- Curates the risk register with the aid of our CISO and CEO
- Reviews the progress made on the various risks with the CEO and CISO on a monthly basis
- Uses the Risk Register as well as meeting minutes to inform annual memo to the Board of Trustees
- Performs a detailed annual walk-through of the risk register with the entire Board of Trustees **(new!)**

Conclusions

- "Risk" is a nebulous concept and there are a lot of subtle moving parts to keep in mind.
- Without writing things down and prioritizing them using some kind of metric (in the case of risk, likelihood x impact), there's no way to keep all of them in one's mind at once.
- Taking an active and thoughtful approach to managing risk is a core part of good governance and indicative of organizational health and maturity.


ARIN 55
POWERED BY PARTICIPATION
Questions and Comments?
Thank you