

# **DRAFT - Charter for the Risk & Cybersecurity Committee**

## **1.0. Purpose**

The Risk & Cybersecurity Committee is established to assist the ARIN Board and ARIN Management in fulfilling its oversight responsibilities by reviewing and reporting on organizational risk issues and cybersecurity risks and mitigation steps.

## **2.0. Composition of the Committee**

The Committee shall consist of three elected members from the Board of Trustees, with one appointed as the Committee Chair. The VP, Information Security will serve as a committee liaison in an advisory capacity.

The Board of Trustees, at its first business meeting of each calendar year, shall appoint the members of the Committee. Members may serve successive one-year terms if they continue to meet the selection criteria. Vacancies on the Committee during a term shall be filled in the same manner as the regular selection process.

When requested, the General Counsel provides advice to the Risk & Cybersecurity Committee.

## **3.0. Scope of Responsibilities**

The Committee has responsibilities in two overall areas: Risk Assessment and Cybersecurity. The Committee shall periodically report to the Board those recommendations that result from fulfilling these responsibilities. It also can hire outside, independent experts for opinions on ARIN's risks as needed.

At the end of each year, the Risk & Cybersecurity Committee shall review its Charter and its performance as a Board committee. Any recommendations from this review shall be reported to the Board of Trustees for consideration.

### **3.1. General Responsibilities**

1. Oversee the evaluation of strategic risks (including emerging risks presented by economic, societal, environmental, regulatory, geo-political, competitive landscape or other conditions, and the business opportunities arising from such emerging risks) by engaging management in an ongoing risk tolerance dialogue as conditions and circumstances change and new opportunities arise.
2. Providing oversight of any risk tolerance statement adopted by ARIN, including the assessment of business performance within the parameters of such a statement.
3. Institute and oversee special investigations as needed and receive reports on litigation and fraud.

4. Review ARIN's director and officer insurance program to ensure appropriate coverage and that all insurance terms and conditions are being met.
5. Perform other activities related to this charter as requested by the board.

### **3.2. Risk Management and Assessment Responsibilities**

1. Review the ARIN Risk Register quarterly and make recommendations as appropriate to the Board of Trustees for improvements to risk management mitigation.
2. In the first half of each year, review ARIN's overall long-term risk profile and provide a report to the Board of Trustees of any recommended changes to ARIN's Strategic Direction to better position the organization to mitigate future risk.

### **3.3. Cybersecurity Responsibilities**

1. Review ARIN Management's report on ARIN's Cyber insurance policies to ensure appropriate coverage and that all insurance terms and conditions are being met.
2. Provide a Cybersecurity Risk Assessment Report to the Board that covers systems and processes relating to ARIN's cybersecurity program.
3. Review ARIN's cybersecurity and other information technology (IT) risks, controls, and procedures, including high level reviews of:
  - a. the threat landscape facing ARIN and ARIN's strategy to mitigate cybersecurity risks and potential breaches.
  - b. data governance and privacy policies,
  - c. incident response and disaster recovery readiness,
  - d. compliance and audits,
  - e. disclosure and reporting requirements and practices.

### **3.4 Reporting Responsibilities**

1. Report at least quarterly to the board about committee activities, issues, and related recommendations.
2. Review any other reports ARIN issues that relate to committee responsibilities.

### **4.0 Committee Logistics**

The Committee will meet at least quarterly. With support from staff the Committee chair will develop an agenda in advance of each meeting. The meeting minutes will include an attendance record and a report of Committee discussions with documented recommendations and decisions. These minutes will be completed, reviewed, and posted no more than three weeks following the meeting.