

Charter for the Risk & Cybersecurity Committee

1.0. Purpose

The Risk & Cybersecurity Committee is established to assist the ARIN Board in fulfilling its oversight responsibilities by working with ARIN Management to review, and report to the Board on, organizational risk issues and cybersecurity risks and mitigation steps. The Committee shall only be delegated the powers and authority, if any, from the Board as specified below; and for any other work or matters requested by the Board, the Committee will work to refer any actions or information for consideration by the Board.

2.0. Composition of the Committee

The Committee shall include three elected members from the Board of Trustees, with one appointed as the Committee Chair. The senior-most ARIN employee responsible for day-to-day risk assessment, mitigation, and governance (if not a Committee member) and for information security, respectively, will serve as committee liaisons in an advisory capacity, and the General Counsel shall act in an advisory capacity upon the Committee's request.

The duties of the Committee Chair include the following:

- prepare for and facilitate committee meetings, including working with staff to shape meeting agendas,
- able to run a meeting, to time, and bring a group to a consensus,
- able to draw on colleagues' skills and abilities,
- able to deploy people management skills to handle different people and personalities, managing the strong versus the quiet, gathering input from all,
- able to establish and maintain a good working relationship with the Board Chair,
- act as subject matter expert and/or offer technical skills related to the committee's mandate.

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.

3.0. Scope of Responsibilities

The Committee has responsibilities in two overall areas: *Risk Identification and Assessment*; and *Cybersecurity*. The Committee shall periodically report to the Board those observations and recommendations, including recommendations relating to mitigation, that result from fulfilling these responsibilities. It may also 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

The Committee shall:

1. Oversee the identification, assessment, and presence of appropriate mitigation approaches for strategic risks (including emerging risks presented by economic, societal, environmental, regulatory, geo-political, and competitive landscapes, and the business requirements arising from such emerging risks) by engaging management in an ongoing risk tolerance dialogue as conditions and circumstances change and new requirements 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 emerging statutory obligations, litigation activity, and any instances of 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 mitigation.
2. In the first half of each year, review ARIN's overall long-term risk profile and report to the Board of Trustees on any recommended changes to ARIN's strategic direction to better position the organization to mitigate future risk.
3. Provide oversight of board-level incident response exercises.

3.3. Cybersecurity Responsibilities

The Committee shall:

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 reviews ARIN's cybersecurity systems and processes, including external compliance standards and audit processes.
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

The Committee shall:

1. Report at least quarterly to the board about committee activities, issues, and related recommendations including a formal summary review of the Risk Register,
2. Report annually to the board, the reports identified in sections 3.2 (long-term risk profile) and 3.3 (cybersecurity risk assessment report) herein.
3. 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.