The ICANN GNSO “Business Constituency”

ICANN Business Constituency (BC) Comment on

The Second Draft of the RIR Governance Document

7-Nov-2025

Background

This document provides input from the ICANN Business Constituency (BC), from the perspective of business users and registrants. We advocate for ICANN policy that:

1. promotes end-user confidence because it is a safe place to conduct business
2. is competitive in the supply of registry and registrar and related services
3. is technically stable, secure and reliable.

General Comment:

Regional Internet Registries (RIRs) play a crucial role in internet governance by managing the allocation and registration of Internet Number Resources, such as IP addresses and Autonomous System Numbers, within specific geographic regions. Their significance lies in ensuring the fair, efficient, and secure distribution of these critical resources, which are essential for the operation and connectivity of the global internet — a foundation that directly supports business continuity, digital innovation, and user trust, which the BC strongly advocates for.

The security practices of RIRs are crucial because they help protect the integrity and availability of the Internet Numbers Registry System. Effective security measures prevent unauthorized access, data breaches, and other cyber threats that could disrupt internet services or compromise sensitive information. By maintaining robust security practices, RIRs ensure the stability and reliability of internet infrastructure, which is vital for the global internet community.

Additionally, secure operations by RIRs help maintain trust among stakeholders, including governments, businesses, and end-users, in the management of internet resources. It is essential for RIRs to maintain robust security practices, particularly in relation to their role in Resource Public Key Infrastructure (RPKI), because RPKI is a critical component in securing the global routing infrastructure of the internet. RPKI helps prevent route hijacking and other malicious activities by providing a way to verify the authenticity and legitimacy of IP address allocations and their associated routes. If

RIRs do not implement strong security measures, the integrity of RPKI could be compromised, leading to potential disruptions in internet connectivity and trust issues within the global internet community. Robust security practices ensure that RIRs can effectively manage and protect the RPKI system, thereby maintaining the stability and reliability of internet operations worldwide.

Recognition and Governance Structure

1. The definition of “Control” (Article 1.1) doesn’t adequately prevent indirect influence through affiliates or proxies. The interpretation here should be limited only to the contracting RIR members and not proxies as a coordinated group could capture the Governing Body by manipulating membership registration or voting, effectively hijacking the RIR’s decision-making process.

2. The governance document can do with more Safeguards Against Governance Capture. For instance, sections: Article 4.1(g), (o); Article 2.3(b)(i)(B) of the draft document only requires that “the majority of an RIR’s Governing Body must be elected by Members”. Here bodies looking to influence outcomes could game the system by onboarding members simply to swing votes. Members so desiring should be financial members up to a certain period, should be financially up-to-date, cover a membership spread amongst regions, etc. thus without stipulating term limits, independent oversight, or diversity requirements, No explicit safeguards exist to prevent member stacking, vote-buying, or mass creation of shell members.

Operational and Security Requirements

RIRs can enhance their cybersecurity framework by adopting and regularly updating an enterprise security risk management program based on internationally recognized standards like NIST or ISO 27001 through the following steps:

- Risk Assessment and Management: Conduct regular risk assessments to identify potential cybersecurity threats and vulnerabilities. Use the findings to develop a risk management plan that prioritizes risks based on their potential impact and likelihood.

- Implementation of Security Controls: Adopt security controls as outlined in standards like NIST or ISO 27001. This includes implementing technical, administrative, and physical controls to protect information assets and ensure the confidentiality, integrity, and availability of data.

- Continuous Monitoring and Improvement: Establish a continuous monitoring process to detect and respond to security incidents promptly. Regularly review and update security policies and procedures to adapt to new threats and changes in the regulatory environment.

- Training and Awareness: Provide ongoing cybersecurity training and awareness programs for employees and stakeholders. This helps in building a security-conscious culture and ensures that everyone understands their role in protecting the organization's information assets.

- Incident Response Planning: Develop and maintain an incident response plan that outlines the procedures for responding to and recovering from cybersecurity incidents. Regularly test and update the plan to ensure its effectiveness.

- Collaboration and Information Sharing: Engage in collaboration and information sharing with other RIRs and relevant cybersecurity organizations. This can enhance threat intelligence and improve the ability to respond to emerging threats.

- Regular Audits and Reviews: Conduct regular audits and reviews of the cybersecurity framework to ensure compliance with the adopted standards and identify areas for improvement.

By incorporating these elements, the RIR Governance Document can strengthen its focus on cybersecurity, ensuring that RIRs are well-prepared to handle the evolving threat landscape and continue to provide secure and reliable services.

In light of the above, the Business Constituency (BC) recommends the following enhancements to the RIR Governance Document:

Article 4: Ongoing Commitments

4.1. Operational Requirements
Enterprise security risk management plan – RIRs must formalize and adopt a comprehensive enterprise security risk management program based on recognized cybersecurity frameworks such as the NIST CSF or ISO 27001.

I. Regular Risk Assessments: Conduct regular risk assessments to identify and evaluate potential cybersecurity threats and vulnerabilities.
II. Continuous Monitoring: Implement continuous monitoring of systems and networks to detect and respond to cybersecurity incidents in real-time. This includes using advanced threat detection tools and techniques.

III. Incident Response Planning: Develop and regularly update incident response plans to ensure quick and effective responses to cybersecurity incidents. This includes conducting regular drills and simulations to test the plans.
IV. Collaboration and Information Sharing: Collaborate with other RIRs, ICANN, and cybersecurity organizations to share threat intelligence and best practices. This collective approach can enhance the ability to anticipate and mitigate threats.
V. Training and Awareness: Provide ongoing cybersecurity training and awareness programs for staff and stakeholders to ensure they are informed about the latest threats and security practices.
VI. Policy and Procedure Updates: Regularly review and update cybersecurity policies and procedures to reflect changes in the threat landscape and technological advancements.
VII. Third-Party Audits: Engage independent third-party auditors to review cybersecurity practices and provide recommendations for improvement.

Oversight, Accountability, and Transparency

3. Improvements to the Oversight Mechanisms highlighted in sections: Article 2.4 (Ad Hoc Audit), Article 4.2 (Audit), Article 6 (Derecognition) can be improved as ICANN's audit powers are reactive ("if requested"), not continuous, leaving gaps until problems become severe. There is also no standing compliance body or automatic trigger for investigation when irregularities arise or governance paralysis are identified before they become full blown. Derecognition is described as a "last resort", but lacks clear, measurable thresholds for arresting the situation before the RIR collapse.

4. Over-Reliance on Unanimity Among RIRs should be treated with caution. The mechanisms as stipulated in sections: Article 2.3(a)(iii)–(v); 2.3(b)(v); 5.1(a) are adequate as it seeks to institute a balance where most critical decisions (Recognition, Derecognition, Emergency Continuity) require unanimous agreement of all RIRs. Thus no single RIR could block necessary action — even if one region is failing — due to political alliances or strategic interests.

5. Ambiguous "Good Faith" and "Reasonable Timeframes" Clauses in sections: Article 2.8, Article 4.1(m), 6.2 have key obligations softened by subjective language such as "reasonable time," "good faith," and "appropriate controls." making enforcement or arbitration difficult when an RIR is deliberately slow or obstructive as bad actors could exploit vagueness to delay compliance, stall audits, or avoid transparency indefinitely under the guise of "reasonableness." However a 90-day window is suggested as a feasible timeline to guide

processes.

6. There is a need to improve Transparency and Accountability Provisions as seen in sections: Article 4.1(k), (q) “Comprehensive records” and “timely manner” are not defined — no minimum transparency requirements (e.g., audited accounts publication deadlines, open board minutes). The dispute resolution clause leaves the design of the mechanism to each RIR, which could result in non-independent or biased arbitration frameworks as an RIR could restrict access to information or manipulate internal dispute systems, shielding misconduct or financial irregularities from community scrutiny.

7. There is a need to provide Limited Protection for Members and Whistleblowers as the entire document lacks explicit protection provisions. There is no mention of whistleblower safeguards, member rights during governance suspension, or anti-retaliation measures. In the case of an existing RIR the absence of the same allowed intimidation and legal harassment against community members and staff who raised concerns.

8. Emergency Continuity Procedure appears too restrictive as seen in sections: Article 5.1(a)–(d) which requires unanimous agreement of other RIRs and ICANN to trigger emergency operations. A 90-day limit may also be inadequate for recovery from deep institutional crises (e.g., legal receivership, frozen accounts, etc.) During crises or a multi-year dysfunction, the system could remain paralyzed because no one can act swiftly without unanimity.

9. Lack of Explicit Financial Transparency Standards as highlighted in sections: Article 4.1(a), (k) through Financial independence is stated, no requirement for public audited statements, independent financial committees, or ICANN verification. No mechanism to detect or prevent embezzlement or misuse of member fees as opaque finances could conceal corruption or political manipulation of budgets.

10. The governance document has no sanctions or progressive discipline model as only two states exist: compliant or derecognized. Grades of graduated sanctions such as warnings, probation, suspension, or partial service transfer and other mechanisms could prevent total collapse. This “all-or-nothing” structure discourages early corrective intervention.

11. Inadequate Regional Legal Risk Mitigation as referenced in sections: Article 4.1(d), 6.3(a) The document assumes legal compliance but does not account for

local court interference or injunctions. There is a need to infuse a global framework in the form of ESCROW services to protect registry data or continuity against domestic court orders. A bad actor could use local legal systems to freeze assets, block board operations, or seize registry control.

Conclusion

The Business Constituency (BC) supports efforts to strengthen the governance and accountability of Regional Internet Registries (RIRs), noting their vital role in maintaining global internet stability. From a business perspective, this framework should include clearer safeguards against governance capture, defined derecognition criteria, and stronger oversight mechanisms. RIRs must also adopt robust, auditable security standards—such as NIST or ISO 27001—to ensure trust, transparency, and operational integrity. These measures will help preserve stakeholder confidence, prevent abuse, and align RIR operations with the accountability expectations of the global business community.

This comment was drafted by Selli Claudia and Lawrence Olawale-Roberts. It was approved in accordance with our Charter.