Declaration of Commitment to International Standards

Consejo Internacional para la Lucha contra la Corrupción, Asociación Civil

Preamble

Consejo Internacional para la Lucha contra la Corrupción, Asociación Civil ("CILC") hereby issues this **Declaration of Commitment to International Standards** as a formal expression of its institutional principles, operational discipline, and unwavering commitment to internationally recognized frameworks governing **quality, sustainability, ethical conduct, information security, and anti-corruption**. This Declaration is intended to articulate, in clear and binding terms of organizational intent, the standards by which CILC governs its internal conduct, engages with stakeholders, and evaluates the integrity of its operational and strategic decisions.

CILC affirms that its activities shall be conducted in a manner consistent with the **highest standards of professionalism, accountability, transparency, and lawful governance**. The organization recognizes that credibility in humanitarian, advisory, and support-oriented work depends not merely upon stated values, but upon demonstrable compliance with rigorous standards that protect the dignity of persons, preserve institutional trust, and ensure responsible stewardship of all resources entrusted to its care. Accordingly, CILC commits to maintaining a framework of operations that reflects **measurable quality assurance, continuous improvement, ethical responsibility, and verifiable control mechanisms** across all relevant functions.

In furtherance of this commitment, CILC declares its alignment with applicable international standards and best practices, including, where relevant to its functions and operational scope, internationally recognized frameworks concerning **quality management, environmental responsibility, occupational integrity, information security, privacy protection, business continuity, and anti-bribery and anti-corruption controls**. This alignment shall not be construed as a mere aspirational reference. Rather, it represents a structured and ongoing organizational obligation to ensure that policies, procedures, decision-making processes, and monitoring mechanisms are designed, implemented, reviewed, and improved in a manner that is consistent with such standards and with the requirements of applicable law.

CILC further declares its commitment to pursuing **independent third-party assessments, audits, accreditations, and certifications** where such mechanisms are appropriate, available, and aligned with the organization’s mission and operational realities. The purpose of such pursuit is to ensure that statements of compliance are supported by credible external validation and that institutional claims are substantiated by objective review. CILC understands that certification is not an end in itself, but a formal instrument of assurance, demonstrating that the organization’s systems and

practices meet defined requirements and remain subject to continual scrutiny. In this respect, CILC regards external verification as an essential safeguard of institutional integrity and as a practical expression of its duty to serve with precision, diligence, and moral seriousness.

CILC unequivocally affirms its **zero-tolerance position toward corruption, fraud, bribery, coercion, deception, abuse of authority, concealment of material facts, and any conduct that may undermine ethical governance or compromise public trust**. The organization shall not knowingly participate in, condone, facilitate, or benefit from any activity that would violate applicable anti-corruption laws, international conventions, professional ethics, or internal compliance obligations. All personnel, representatives, contractors, consultants, affiliates, and other persons acting on behalf of CILC are expected to uphold this standard without exception. Ethical conduct shall be treated as a core operational requirement, not a discretionary ideal.

In addition, CILC recognizes that **information security, confidentiality, privacy, and responsible data governance** are indispensable to lawful and trustworthy operations. The organization undertakes to maintain appropriate technical, administrative, and organizational safeguards designed to protect sensitive information, prevent unauthorized access, limit the risk of loss or misuse, and ensure that information is processed only for legitimate, authorized, and proportionate purposes. CILC further commits to ensuring that all data-handling practices reflect the principles of necessity, integrity, accountability, and respect for the rights and legitimate interests of affected persons.

CILC also affirms its commitment to **sustainability and responsible conduct**, recognizing that institutional excellence extends beyond immediate operational outcomes and includes long-term responsibility toward people, communities, and the broader environment in which the organization functions. Where applicable, CILC shall seek to integrate sustainable practices into procurement, logistics, service delivery, and internal administration, in a manner that is consistent with legal obligations, ethical expectations, and the prudent management of resources.

This Declaration shall be interpreted as a formal statement of organizational policy, intent, and governing principle. It shall guide the development and implementation of internal controls, compliance programs, staff conduct standards, vendor expectations, risk management procedures, and corrective action mechanisms. CILC expects all internal and external stakeholders to understand that compliance with international standards is not treated as a symbolic aspiration, but as a **substantive operational requirement** that informs the organization’s identity, reputation, and accountability.

Accordingly, CILC declares that it will **continuously review, strengthen, and refine its systems and practices** in order to preserve alignment with evolving international standards, applicable legal requirements, and recognized ethical norms. This Declaration reflects a lasting commitment to institutional excellence, lawful integrity, and uncompromising moral responsibility.

I. APPLICABLE ISO STANDARDS

The following ISO standards constitute a foundational component of **Consejo Internacional para la Lucha contra la Corrupción, Asociación Civil (CILC)** corporate governance, operational discipline, and compliance architecture. They are applied not as isolated certifications or symbolic benchmarks, but as **binding internal standards of conduct**, integrated into policy design, executive oversight, risk management, procurement, training, monitoring, and corrective action processes. CILC's approach is grounded in the principle that **responsible operations are inseparable from lawful operations**, and that organizational credibility depends upon **documented, measurable, and independently verifiable compliance**. Where a standard is certifiable, CILC is pursuing formal certification through structured implementation and external assessment; where a standard is advisory in nature, CILC has adopted its principles as mandatory governance criteria and is pursuing formal alignment validation accordingly.

A. ISO 26000:2010 — Social Responsibility

Standard Reference: ISO 26000:2010, *Guidance on Social Responsibility*
Official Source: https://www.iso.org/iso-26000-so...

CILC's social responsibility framework is guided by the core principles of ISO 26000, including **accountability, transparency, ethical behavior, respect for stakeholder interests, respect for the rule of law, respect for international norms of behavior, and respect for human rights**. In operational terms, this means that CILC does not treat social responsibility as a public relations function or a discretionary goodwill initiative; rather, it is embedded into **strategic planning, internal governance, policy formulation, performance evaluation, vendor engagement, and community-facing activities**. CILC recognizes that responsible institutions must demonstrate not only legal compliance, but also a sustained commitment to **human dignity, fair treatment, non-discrimination, labor integrity, and social value creation**.

In practice, CILC's implementation addresses the principal subjects identified by ISO 26000, namely **organizational governance, human rights, labor practices, the environment, fair operating practices, consumer-related responsibility, and community involvement and development**. Particular emphasis is placed on stakeholder identification and engagement, grievance awareness, ethical decision-making, and the prevention of harm through proactive governance rather than reactive remediation. CILC's internal structure is designed to ensure that leadership decisions are informed by **social impact, legal risk, reputational consequence, and the moral obligations owed to employees, clients, partners, and affected communities**.

It is important to note that ISO 26000 is a guidance standard and is not intended for certification. Accordingly, CILC's position is not one of formal certification under this standard, but of full substantive alignment supported by internal audit, third-party assessment, and continuous improvement mechanisms. Implementation status: an internal self-assessment against the guidance is planned for the second half of 2026, with a management review to follow in 2027. CILC's

objective is to ensure that its social responsibility framework is not merely declared, but demonstrably embedded, independently reviewed, and consistently enforced.

B. ISO 14001:2015 — Environmental Management Systems

Standard Reference: ISO 14001:2015, *Environmental Management Systems*
Official Source: https://www.iso.org/iso-14001-en...

CILC maintains an environmental management approach aligned with ISO 14001 that is designed to identify, control, monitor, and continually improve the organization's environmental performance across all relevant operations and jurisdictions. This framework covers **greenhouse gas emissions, energy consumption, waste generation and diversion, water use, procurement impacts, environmental compliance obligations, and supply chain environmental performance**. CILC's environmental governance is founded on the principle that environmental responsibility is not optional, peripheral, or reputationally convenient; it is a **non-negotiable operational duty** that must be discharged through traceable systems, measurable objectives, and accountable leadership.

CILC applies the **Plan-Do-Check-Act (PDCA)** cycle as the structural basis for environmental management. This includes the establishment of annual environmental objectives, performance indicators, compliance controls, management review procedures, and corrective action pathways. Environmental risk is assessed not only in relation to direct operations, but also through lifecycle considerations and upstream/downstream dependencies where CILC's activities may influence environmental outcomes. The organization's approach includes measures aimed at **pollution prevention, resource efficiency, operational resilience, sustainable procurement, and compliance with applicable environmental laws and permit conditions**. CILC also ensures that environmental responsibilities are assigned clearly, recorded appropriately, and reviewed at a level sufficient to support executive accountability.

Implementation status: an environmental baseline review is planned for the second half of 2026; ISO 14001 certification is targeted for 2027. The certification scope includes headquarters and all major operational facilities across jurisdictions, subject to local legal applicability and operational relevance. CILC's environmental management system is intended to satisfy not only the formal criteria of ISO 14001, but also the broader expectation that an institution of integrity must act with discipline, restraint, and responsibility toward the ecological consequences of its conduct.

C. ISO 27001:2022 — Information Security Management Systems

Standard Reference: ISO 27001:2022, *Information Security Management*
Official Source: https://www.iso.org/iso-27001-in...

CILC's information security governance is structured to protect the **confidentiality, integrity, and availability** of information assets, including personal data, operational records, strategic

documentation, and other sensitive information entrusted to the organization. In a climate of escalating cyber risk, regulatory scrutiny, and transnational data exposure, CILC treats information security as a matter of **institutional survival, legal compliance, and ethical responsibility**. The organization's controls are therefore built around a risk-based framework that is both preventive and responsive, ensuring that access, processing, storage, transmission, and disposal of information are governed by clear rules, documented procedures, and auditable oversight.

CILC's information security system encompasses **personnel security, asset classification, access control, cryptographic safeguards, secure configuration, logging and monitoring, incident management, business continuity, supplier security, and data handling discipline**. Particular attention is given to the protection of personal and confidential data, the prevention of unauthorized disclosure or alteration, and the rapid containment of security incidents when they occur. CILC also recognizes that security is not achieved through technology alone. It requires **trained personnel, accountable leadership, procedural rigor, and an organizational culture that rejects negligence, concealment, and complacency**. The system therefore incorporates awareness training, access governance, incident escalation channels, response protocols, and post-incident review mechanisms designed to produce continual strengthening of controls.

Implementation status: an information security risk assessment and gap analysis are planned for the second half of 2026; ISO 27001 certification is targeted for 2027. CILC's objective is not merely to satisfy the minimum threshold of compliance, but to establish a resilient, defensible, and continuously improving security posture capable of withstanding legal, operational, and reputational challenges. In all respects, CILC's position is that the protection of information is a duty of trust, and any failure in this domain must be treated with seriousness, transparency, and immediate corrective action.

D. ISO 37001:2016 — Anti-Bribery Management Systems

Standard Reference: ISO 37001:2016, *Anti-Bribery Management Systems*
Official Source: https://www.iso.org/iso-37001-an...

CILC's anti-bribery and anti-corruption framework is aligned with ISO 37001 and reflects a **zero-tolerance position toward bribery, corruption, facilitation payments, undue influence, and any conduct that compromises integrity or distorts fair dealing**. CILC regards bribery not as a mere compliance issue, but as a direct assault on lawful governance, institutional legitimacy, and moral order. Accordingly, the organization's anti-bribery controls are designed to prevent, detect, investigate, and remediate corrupt conduct across all activities, including interactions with public officials, private-sector counterparties, intermediaries, vendors, consultants, and other third parties acting on CILC's behalf or in connection with CILC's interests.

CILC's anti-bribery management system includes **risk assessment, due diligence on third parties, controls over gifts and hospitality, conflicts-of-interest management, training and awareness, confidential reporting mechanisms, investigation protocols, disciplinary measures, and remediation procedures**. The framework is intended to ensure that suspicious

activity is escalated promptly, investigated impartially, and addressed with consequences proportionate to the severity of the breach. CILC further ensures that anti-bribery obligations are communicated clearly to personnel and counterparties, and that compliance expectations are integrated into contracting, onboarding, procurement, and oversight practices. The organization does not accept ambiguity where integrity is required; it demands **clarity, accountability, documentary traceability, and decisive enforcement**.

Implementation status: an anti-bribery self-assessment is planned for the second half of 2026; ISO 37001 certification is targeted for 2027. CILC's commitment is to maintain an anti-bribery framework that is not merely compliant in form, but credible in substance, enforceable in practice, and uncompromising in ethical standard. Any deviation from this standard is treated as a serious governance failure requiring immediate review and corrective action.

II. CERTIFICATION ROADMAP & TIMELINES

Consejo Internacional para la Lucha contra la Corrupción, Asociación Civil is committed to the orderly, verifiable, and independently validated implementation of a certification program that demonstrates institutional integrity, operational discipline, and measurable compliance across the organization's core governance domains. The certification roadmap set out below is not a symbolic declaration of intent; it is a **structured compliance sequence** designed to ensure that each certification is pursued on the basis of **documented readiness, auditable evidence, formal management oversight, and external verification by accredited bodies**.

The organization's approach to certification is governed by the principle that **no certification shall be treated as achieved until it has been formally issued by an accredited independent certification body recognized by the relevant national accreditation authority**. Internal assessments, gap analyses, baseline audits, and alignment reviews are therefore treated as preparatory and control-building mechanisms only. They are essential to readiness, but they are **not substitutes for certification**. This distinction is fundamental to the organization's ethical posture and legal precision. It ensures that all public, regulatory, and stakeholder-facing references to compliance remain **accurate, conservative, and defensible**.

The roadmap reflects a staged progression across the major operational risk areas most relevant to a modern professional institution: **anti-bribery compliance, environmental governance, social responsibility, and information security**. Each standard has been selected not merely for reputational value, but because it corresponds to a distinct and material category of organizational risk. The certification timetable has therefore been designed to permit meaningful remediation, internal control reinforcement, management review, and third-party assessment within a realistic and accountable implementation window.

ISO Standard	Target Certification Date	Current Status	Auditor Assignment

ISO 37001 (Anti-Bribery)	**2027**	**Self-assessment planned**	**TBD**
ISO 14001 (Environmental Management)	**2027**	**Baseline review planned**	**TBD**
ISO 26000 (Social Responsibility)	**2027**	**Self-assessment assessment in progress**	**TBD**
ISO 27001 (Information Security Management)	**2027**	**Gap analysis planned**	**TBD**

ISO 37001 (Anti-Bribery) is treated as a priority control standard because it directly addresses the organization's commitment to zero tolerance for bribery, improper inducements, facilitation payments, concealment mechanisms, and any form of corrupt influence. A planned self-assessment will initiate the structured verification of its anti-bribery framework, including governance controls, reporting channels, third-party integrity expectations, and procedural safeguards. The target certification date in 2027 reflects the organization's intent to move promptly from internal validation to external certification, subject to final closing of any audit observations and confirmation of certification-body scheduling. In this context, audit completion is not the endpoint; it is the evidentiary foundation for independent certification.

ISO 14001 (Environmental Management) is being advanced through a baseline audit to establish the organization's current environmental footprint, applicable legal obligations, risk exposures, operational dependencies, and opportunities for continual improvement. This standard requires more than general environmental awareness; it requires a demonstrable management system capable of identifying, controlling, monitoring, and improving environmental performance in a disciplined and measurable manner. The target certification date of **2027** is aligned with the time required to assess existing environmental practices, formalize objectives and controls, and ensure that the system is sufficiently mature for external evaluation. The organization will proceed only on the basis of **documented compliance evidence** and **verifiable performance controls**, rather than aspirational statements.

ISO 26000 (Social Responsibility) is being approached as a strategic alignment exercise rather than a narrow compliance instrument, because its value lies in its ability to articulate the organization's responsibility toward **ethical conduct, stakeholder respect, human rights awareness, fair practices, transparency, and accountability**. While ISO 26000 is guidance-based rather than certifiable in the same manner as certain management system standards, the organization is nevertheless treating it with full seriousness as a benchmark for institutional behavior and policy coherence. The current alignment assessment is designed to determine the degree to which existing policies, governance mechanisms, workforce expectations, and stakeholder commitments correspond to recognized principles of social responsibility. The target date of **2027** reflects a deliberate and methodical process of refinement, consultation, and internal harmonization before any external assurance or public positioning is considered.

ISO 27001 (Information Security Management) is being pursued because the protection of information assets is a matter of **institutional resilience, legal exposure, client trust, and operational continuity**. The ongoing gap analysis is intended to identify deficiencies across governance, access control, asset management, incident response, business continuity, supplier assurance, and information risk treatment. This certification is particularly significant because information security failures can create immediate and serious consequences, including regulatory exposure, contractual breach, reputational harm, and compromise of sensitive data. The target certification date of **2027** reflects the need for rigorous remediation, evidence capture, policy integration, staff awareness, and control validation before independent assessment. **Certification in this domain must be earned through demonstrable control maturity**, not asserted through policy language alone.

All certifications shall be obtained exclusively through **accredited independent certification bodies** recognized by the relevant **national accreditation authorities**. This requirement is non-negotiable and serves several essential purposes: it preserves the independence of the assessment process, ensures that findings are technically credible and externally defensible, and guarantees that any issued certificate carries the legitimacy associated with formal accreditation. The organization will not engage in any certification process that compromises auditor independence, circumvents accreditation requirements, or substitutes internal approval for external validation. **Integrity of process is as important as the certificate itself**.

From a governance perspective, the certification roadmap shall be managed as a controlled portfolio of compliance initiatives with clear ownership, scheduled reviews, evidentiary requirements, and escalation protocols. Any delays, nonconformities, or certification-body reservations will be documented and addressed through corrective action plans subject to management oversight. Where necessary, target dates may be refined in order to preserve the organization's commitment to **accuracy, completeness, and certification readiness without premature declaration**. The organization's position is unequivocal: **compliance must be proven, not presumed**.

Note: All certifications will be obtained from **accredited independent certification bodies recognized by national accreditation authorities**, and any public reference to certification status will be made only in a manner that is **factually precise, legally defensible, and consistent with the formal outcome of the external certification process**.

III. COMMITMENT TO CONTINUOUS IMPROVEMENT

Consejo Internacional para la Lucha contra la Corrupción, Asociación Civil ("CILC") hereby affirms that continuous improvement is not a discretionary aspiration, but a mandatory operational principle embedded in the governance, supervision, and execution of all organizational activities. CILC shall maintain a disciplined, systematic, and evidence-based approach to the implementation of ISO-aligned management systems across its functions, ensuring that such systems are not treated as isolated compliance instruments, but as integral mechanisms for institutional integrity, operational reliability, and long-term organizational resilience. **This**

commitment extends to every relevant level of the organization, including leadership, management, administrative operations, service delivery, internal controls, and stakeholder-facing processes.

CILC shall **design, implement, preserve, and continually improve ISO-compliant systems** in a manner consistent with the applicable standards, certification requirements, and recognized best practices governing quality, operational discipline, risk mitigation, and organizational accountability. Such implementation shall not be merely formalistic or procedural in character; rather, it shall reflect a substantive commitment to maintaining processes that are measurable, auditable, and demonstrably effective. **CILC shall ensure that its systems remain current, responsive, and capable of supporting both regulatory compliance and institutional excellence.** Where certification obligations are identified, CILC shall pursue such certifications within the timelines established by its internal compliance schedule or any external commitment previously communicated, and shall take all reasonable and necessary measures to ensure readiness for third-party assessment, verification, and recognition.

Once obtained, all certifications shall be **actively maintained in good standing** through the full observance of surveillance audit requirements, periodic monitoring obligations, corrective action implementation, and any other conditions imposed by the relevant certification body. CILC recognizes that certification is not a static achievement, but a continuing obligation that requires sustained discipline, documentary integrity, management oversight, and operational accountability. Accordingly, **any nonconformity, weakness, deficiency, or risk identified through audit, review, incident reporting, or internal evaluation shall be addressed promptly, thoroughly, and in a manner proportionate to the seriousness of the issue**, with the objective of preventing recurrence and strengthening system performance. CILC shall not permit compliance to deteriorate through neglect, delay, or superficial remediation.

CILC shall also ensure that **its performance against ISO standards is communicated transparently and responsibly to relevant stakeholders**, including through annual sustainability reporting or equivalent governance reporting instruments, as applicable. Such communication shall be accurate, complete, and capable of substantiation, and shall reflect both achievements and areas requiring further improvement. **Transparency in this context is a duty, not a public relations exercise.** Reporting shall therefore include meaningful information concerning compliance status, certification progress, audit outcomes, key performance indicators, material risks, corrective actions, and strategic measures undertaken to strengthen organizational effectiveness. Where appropriate, CILC shall present this information in a manner that permits stakeholders to assess the seriousness, credibility, and continuity of its commitment to internationally recognized standards.

In furtherance of this obligation, CILC shall use ISO frameworks as a structured foundation for **continuous improvement in organizational effectiveness, risk management, and stakeholder engagement**. This includes the regular identification of process inefficiencies, operational vulnerabilities, compliance gaps, and governance weaknesses; the implementation of corrective and preventive actions; and the systematic review of performance trends to ensure that

organizational decisions are informed by evidence rather than assumption. **Continuous improvement shall be understood as a permanent institutional duty**, requiring that CILC not only correct deficiencies when they arise, but actively seek opportunities to refine practices, strengthen internal controls, improve responsiveness, and enhance the quality and consistency of its outputs.

CILC shall further ensure that **all personnel receive appropriate training, instruction, and periodic refresher guidance regarding their respective responsibilities in maintaining ISO compliance**. Training shall be role-specific, current, and sufficiently detailed to enable personnel to understand the standards applicable to their functions, the consequences of noncompliance, the importance of accurate documentation, and the necessity of timely escalation where risks or deficiencies are identified. The organization shall maintain a culture in which compliance is understood not as an administrative burden, but as a professional obligation tied directly to service quality, institutional credibility, and ethical conduct. **No personnel member shall be presumed competent in ISO-related responsibilities absent adequate instruction and demonstrated understanding.**

Finally, CILC shall conduct **annual reviews of all ISO-aligned policies, procedures, controls, and supporting documentation** to ensure that they remain legally sound, operationally effective, and consistent with evolving standards, external requirements, and organizational needs. Such reviews shall be substantive rather than ceremonial, and shall assess whether existing policy architecture continues to reflect the organization's actual risk profile, operational scope, stakeholder obligations, and compliance commitments. Where revision is necessary, CILC shall update its policies promptly, formally approve the revised instruments through the appropriate governance channel, and communicate the changes to affected personnel without delay. **The organization shall not tolerate outdated policies, inconsistent practice, or avoidable ambiguity where clarity, accountability, and precision are required.**

Accordingly, CILC declares that continuous improvement shall remain a standing organizational obligation, to be pursued with rigor, transparency, and unwavering commitment to compliance, operational excellence, and stakeholder trust. This commitment shall be implemented in good faith, enforced without exception, and reviewed continuously to ensure that CILC remains aligned with the highest standards of professional conduct and ISO governance.

IV. EXTERNAL VALIDATION & MONITORING

Consejo Internacional para la Lucha contra la Corrupción, Asociación Civil shall maintain a rigorous, continuously verifiable framework of **external validation, internal oversight, and management accountability** to ensure that its ISO-aligned governance system remains **certifiable, effective, traceable, and fully compliant** at all times. Certification shall not be treated as a symbolic designation or a one-time achievement, but as a **continuing obligation of institutional discipline**, requiring sustained evidentiary support, documented control, timely correction, and transparent accountability. The organization expressly recognizes that the

credibility of its compliance posture depends not on declarations of conformity, but on the **objective demonstrability of conformity through audited evidence, corrective action, and responsible leadership oversight**.

1. Independent Certification Audits.

All certification audits shall be conducted exclusively by **accredited external auditors** acting in accordance with the applicable ISO certification requirements and the procedures established by the relevant certification body. These audits shall evaluate, without limitation, the design, implementation, operational control, and sustained effectiveness of the organization's management system, including its policies, procedures, records, governance mechanisms, risk controls, and evidence of continual improvement. Consejo Internacional para la Lucha contra la Corrupción, Asociación Civil shall provide auditors with full, timely, lawful, and unimpeded access to the information, personnel, locations, and records reasonably required for an impartial assessment. The organization shall preserve the integrity of all evidence, prohibit any interference with auditor independence, and ensure that any identified nonconformity is addressed through documented corrective action within the timeframes prescribed by the certification framework. **No certification claim shall be asserted, maintained, or implied unless it is supported by current, valid, and verifiable audit evidence**. Where deficiencies are identified, they shall not be minimized, obscured, or normalized; they shall be treated as formal compliance matters requiring immediate attention, responsible ownership, and documented remediation.

2. Surveillance Audits.

During the certification cycle, **surveillance audits** shall be conducted on an annual or biennial basis, strictly in accordance with the schedule, scope, and methodology determined by the certification body. The purpose of such audits is to verify that the management system continues to operate in practice as represented in policy, procedure, and record, and that the organization has maintained not merely initial compliance, but **sustained compliance over time**. Surveillance audits shall examine whether previous findings were effectively resolved, whether corrective actions remain durable, and whether any emerging risks, operational deviations, or control weaknesses indicate a deterioration in compliance performance. The organization shall regard each surveillance audit as a substantive test of integrity, not as a procedural formality. Any observation, nonconformity, or pattern of weak control shall be escalated promptly to senior management, documented without distortion, and resolved through measurable corrective action. **Ongoing certification depends upon continuous conformity, not historical performance**; accordingly, any material lapse in governance, documentation, implementation, or oversight shall be treated as a serious institutional failure requiring immediate remedial discipline.

3. Internal Audits.

Consejo Internacional para la Lucha contra la Corrupción, Asociación Civil shall conduct **quarterly internal audits** of all ISO-aligned processes, controls, records, and obligations within the scope of its management system. These audits shall be performed by qualified personnel

operating with sufficient independence from the activity under review to preserve objectivity and credibility, and shall be grounded in documented criteria, evidence-based assessment, and risk-sensitive prioritization. Internal audit findings shall be recorded with precision, classified according to their severity, impact, and corrective urgency, and communicated through an accountable internal process that ensures action rather than mere notation. Every nonconformity, weakness, or process deviation shall be assigned a responsible owner, a defined deadline, and a clear corrective plan that addresses both the immediate issue and its root cause. The organization shall not consider a finding closed until it has verified, through documented evidence, that the correction has been implemented, the underlying cause has been addressed, and the risk of recurrence has been reduced to an acceptable and demonstrably controlled level. **Internal audit is not an administrative exercise; it is a core mechanism of institutional self-discipline, early detection, and compliance preservation**.

4. Management Review and Stakeholder Reporting.

At least annually, senior leadership shall conduct a formal **management review** of the ISO system's suitability, adequacy, effectiveness, and strategic alignment. This review shall consider, at minimum, audit outcomes, nonconformity trends, the timeliness and effectiveness of corrective actions, compliance risks, stakeholder concerns, process performance, and opportunities for systemic improvement. The review shall produce documented decisions, assigned responsibilities, and tracked action items until completion, with follow-up sufficient to confirm that leadership oversight is not aspirational but operationally real. In parallel, the organization shall ensure **transparent stakeholder reporting** through its annual reports or equivalent formal disclosures, publishing a truthful, accurate, and balanced account of certification status, significant audit findings, corrective measures undertaken, and the organization's demonstrated progress in compliance maturity. Such reporting shall be complete enough to evidence accountability and integrity, while remaining consistent with lawful confidentiality, data protection, security obligations, and any other binding restrictions. **Transparency is a duty of trust, not a marketing choice**; accordingly, the organization shall not obscure material compliance matters, dilute adverse findings, or present corrective action as complete before it has been objectively verified.

Consejo Internacional para la Lucha contra la Corrupción, Asociación Civil shall therefore apply a **zero-tolerance standard toward superficial compliance, undocumented claims, and unverified remediation**. Its external validation and monitoring system shall function as a permanent safeguard of credibility, ensuring that certification remains substantively justified, operationally meaningful, and ethically unimpeachable. The organization's position is unequivocal: **compliance must be real, auditable, and continuously maintained; anything less is unacceptable**.

Signed by:

Dzianis Limarau

President, Consejo Internacional para la Lucha contra la Corrupción, Asociación Civil

Date: 11 September 2026