ISO37002 and How to Operationalize Whistleblowing in the Caribbean

Andrew Samuels CEO WislPort Compliance

June 23rd, 2025

ISO37002 - Introduction

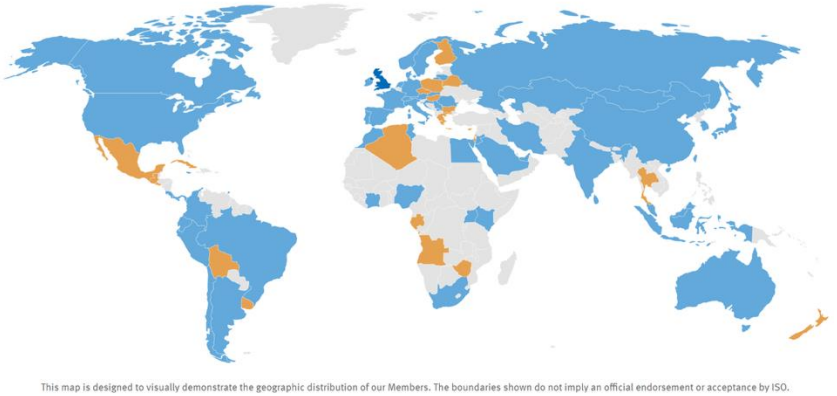
Guidelines for establishing, implementing and maintaining an effective whistleblowing management system based on the principles of trust, impartiality and protection in the following four steps:

a) receiving reports of wrongdoing;
b) assessing reports of wrongdoing;
c) addressing reports of wrongdoing;
d) concluding whistleblowing cases.

applicable to all organizations, regardless of type, size, nature of activity, and whether in the public, private or not-for profit sectors.

Intended outcomes:

- encouraging and facilitating reporting of wrongdoing;
- supporting and protecting whistleblowers and other interested parties;
- ensuring reports of wrongdoing are dealt with in a proper and timely manner;
- improving organization culture and governance;
- reducing the risk of wrongdoing.



161 experts, 35 countries, 7 liaisons

(business, government, union, civil society, whistleblowers)

SUSTAINABLE DEVELOPMENT GOALS

11 16 8

Alignment with Governance

TC309 Governance of Organizations was established in 2016 to establish for the first time an international consensus on the principles of good organizational governance at the international level, in an inclusive, transparent manner and applicable to all types of organizations, all countries, and all sectors.

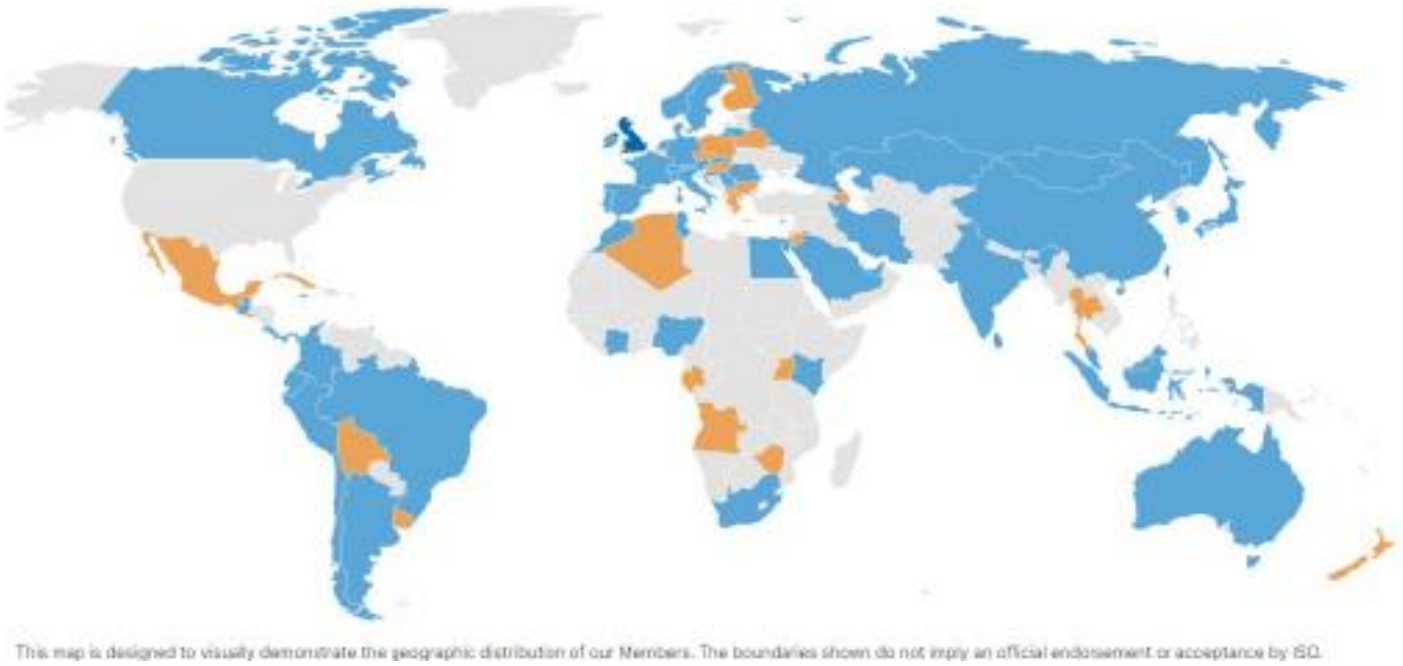
9 Published ISO standards

8 ISO standards under development

59 Participating members

27 Observing members

This committee is the recipient of the 2024 Lawrence D. Eicher Leadership Award



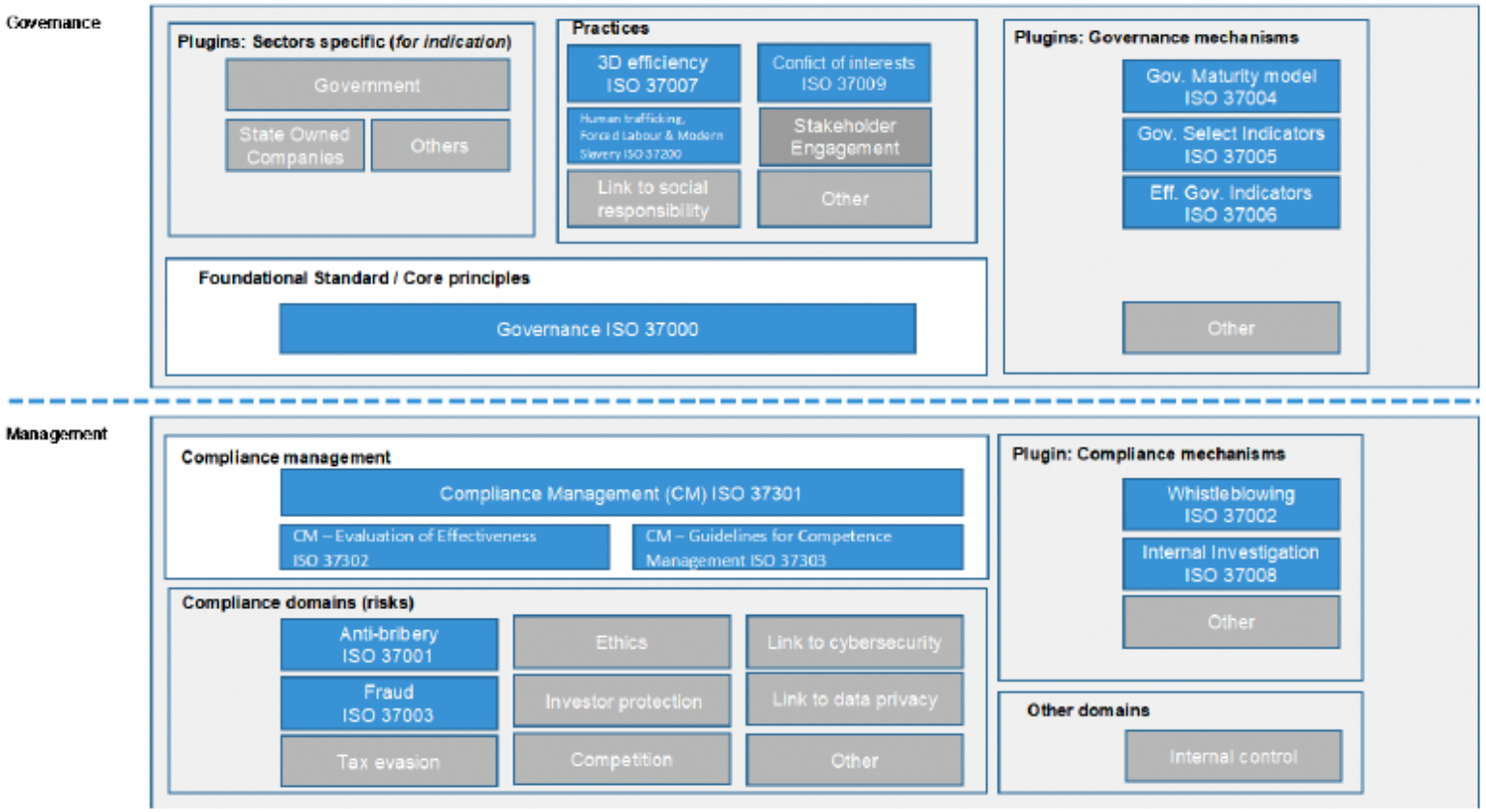
Alignment of ISO37002 with other GRC Standards

ISO TC309 has a strategic focus in Integrated Governance and Compliance.

Whistleblowing is one of the most cost-effective compliance mechanisms for the early detection, prevention, or mitigation of wrongdoing.

It's ability to deliver defence and value also supports key success functions and factors such as risk management and culture.

Understood and applied correctly, ISO37002 aligned whistleblowing programmes can improve culture and reduce exposure to risk and wrongdoing.



Examples

ISO 37000:2021 - Governance of Organizations

Clause 6.2.5 - Accountability: Stresses the importance of establishing mechanisms like whistleblowing channels to ensure accountability and transparency within the organization.

Clause 8.3 - Reporting and Transparency: Encourages organizations to implement confidential reporting (whistleblowing) systems to address governance-related issues and report unethical behavior.

Clause 9.2 - Ethical Culture: Highlights the necessity for organizations to foster a culture of ethical behavior, with mechanisms like whistleblowing systems that allow reporting of misconduct without fear of retaliation.

ISO 37001:2016 - Anti-Bribery Management Systems

Clause 5.3.4 - Raising Concerns and Reporting: Refers to the need for organizations to implement mechanisms, such as whistleblowing channels, to report bribery risks or concerns in good faith.

Clause 8.9 - Raising Concerns: Encourages organizations to provide a confidential reporting system for concerns related to bribery.

ISO 37301:2021 - Compliance Management Systems

Clause 8.2.2 - Communication of Compliance Policies and Procedures: Requires organizations to establish a confidential and accessible whistleblowing mechanism for reporting non-compliance and misconduct.

Clause 8.4 - Confidential Reporting (Whistleblowing): Organizations must ensure that individuals can report compliance breaches or concerns confidentially or anonymously without fear of retaliation.

ISO 31000:2018 - Risk Management

Clause 7.2 - Reporting Mechanisms: References the establishment of channels (such as whistleblowing) to report risks and ensure transparency.

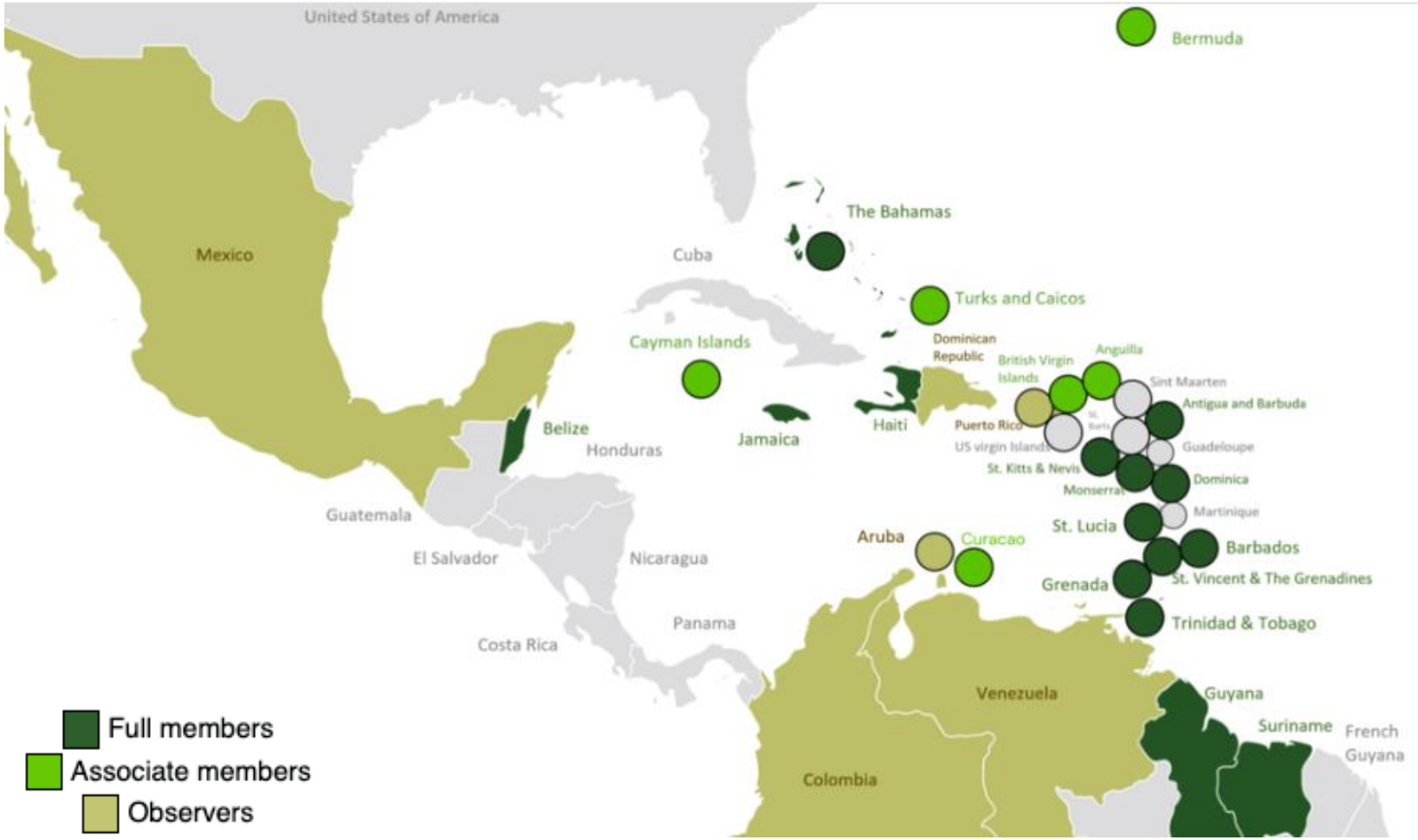
Scope of the Whistleblowing Programme

The scope of the whistleblowing is very much determined by the context of the organisations:

- External and internal issues;
- Legal and regulatory obligations
- Jurisdiction(s)
- Internal and external stakeholders
- compliance risk assessments or equivalent.

- Organizations can reference ISO 37301 for compliance risk assessment and ISO 31000 for risk management.
- The types of wrongdoing that can be addressed through the whistleblowing management system, if reported, are important to its scope.
- Some reports may be made that are outside of the scope such as complaints. It's important to have a process to allocate these correctly.

Applying this to the Caricom Region



Caricom Whistleblowing Laws

- Antigua and Barbuda: Law No. 60/2016 on Whistleblowing and Whistleblower Protection The Bahamas: Protected Disclosures Bill, 2025 (currently a Bill, expected to become law).
- Barbados: Whistleblower Protection Act, 2021.
- Belize: Whistle Blower Act (CAP 527) Act VIII of 2013 as amended by Act LXVII of 2021.
- Grenada: The Data Protection Bill, 2023 includes whistleblower protections related to data violations.
- Guyana: Protected Disclosures Act No. 5 of 2018.
- Jamaica: The Protected Disclosures Act, 2011.
- Saint Kitts and Nevis: Whistleblowers Protection Bill, 2023
- Suriname: Whistleblowers' Protection Law 2018 (No. 83-2018), amended by Law No. 182-2020.
- Trinidad & Tobago: Whistleblower Protection Act, 2024 (Act No. 9 of 2024).

Applying this to the Caricom Region - Anonymity

There's a significant difference between a law allowing an anonymous report to be received and investigated (meaning the information is used) versus a law that provides the full legal protections of a whistleblower to an anonymous individual whose identity is never revealed. Here are three perspectives:

Guyana: Protected Disclosures Act No. 5 of 2018 emphasizes protecting the confidentiality of the whistleblower's identity (Section 19), it does not explicitly prohibit anonymous disclosures. The focus is on protecting "information that identifies or may lead to the identification of the person who has made the disclosure." This language *could* allow for anonymous reports, with the understanding that if the identity is never known, the specific person cannot be "protected" in the same way as someone whose identity is known but kept confidential. However, the information itself can still be acted upon.

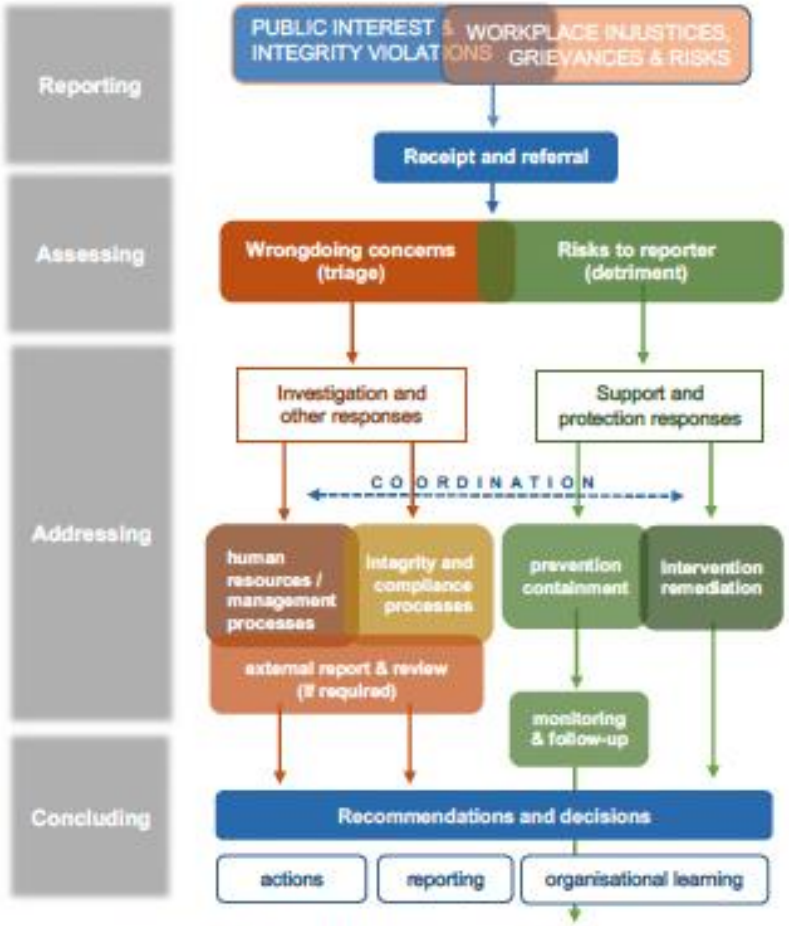
Jamaica: The Protected Disclosures Act, 2011. Official guidelines from the Office of the Services Commissions explicitly state: "Anonymous disclosures are accepted but are not protected by the Act." It goes on to explain that it may be "difficult or impossible to apply" full protections like keeping the discloser informed or protecting them from penalization if their identity is unknown. However, they do state that "reports or concerns of alleged wrongdoings expressed anonymously will be acted upon."

Trinidad & Tobago: Whistleblower Protection Act, 2024 (Act No. 9 of 2024) explicitly addresses anonymous disclosures. Section 7(2) states: "Subject to subsection (3), a whistleblowing reporting officer or whistleblowing reports unit may receive and process an anonymous disclosure and may take the disclosure into account in determining whether improper conduct has occurred." Section 7(4) adds: "Where the identity of a person who makes an anonymous disclosure becomes known, the disclosure shall be deemed to be a protected disclosure if it would have been a protected disclosure if it had not been made anonymously."

Start with the Policy

- Zero tolerance to detriment; Detriment aimed at a person who is known or suspected to have raised a concern should never be tolerated.
- Channels and approach to reporting; Allow for anonymous reports with two-way communication channels. People often reveal themselves once trust has been built
- Approach to anonymity: Be clear – you can't protect a person if you don't know who they are EXCEPT the zero-tolerance clause leads to sanctions for anyone who tries to identify or act against an actual or suspected whistleblower.
- Commitment to follow up on all concerns and feedback in line with data protection and legal requirements. Once evidence has been provided it can't be ignored. Too many firms focus on the source of evidence rather than the evidence itself. Anonymously delivered evidence should be investigated – eve if it means the case handler or organization becoming the Whistleblower

Build Protection into Operations Processes



Source: Brown, Samuels, Kayser & Vandekerckhove (2018)

- Key to a defensible whistleblowing programme is a well-defined process, supported by controls, transparent throughout its lifecycle, and impartial throughout each concerns lifecycle.
- Support and protection is equally as important as the wrongdoing of the concern.
- Each concern presents an opportunity for continual learning and improvement.
- Monitoring and follow up on the well-being of the person raising the concern should go beyond the life of the case.

An organization is only supported and protected when its people are supported and protected

AI – The Hype

Whistleblowing Is about utilizing human intelligence. It's built on empathy and trust. It's about the facts.

- AI is all the talk right now. Yet the current 'AI' offerings are primarily focused on chatbot solutions to allow a whistleblower to ask questions and get a response. It may use AI technology, however there is little to no machine learning to adapt questions in real time.
- Empathy, the ability to ask (and mean) the right questions about a whistleblower's wellbeing can bot build trust AND make it easier to re-call and provide information. It is after all a very personal journey to speak up when something is wrong.
- AI technology (and no technology) can take away the need for human review and approval.

The questions an organization should ask before investing in any solution including an AI solution are:

1. Is this proportionate to the size and complexity of my organization?
2. Do I understand how this works?
3. Will this build trust with our people?
4. Will this build trust with regulators and other stakeholders?

AI – The Opportunity

Whistleblowing Is about utilizing human intelligence. It's built on empathy and trust. It's about the facts.

- AI can be used to impartially and objectively undertake an initial triage with the benefits of quicker human decision making on next steps.
- It can be used in an integrated GRC programme to help identify issues, risks and trends across the organization and industry.
- It can be used to create insights and recommendations for control improvements in compliance.

Ultimately it will require human review, understanding, and signoff. Whistleblowers for the foreseeable future will still be better placed to build trust and empathy with another human – AI can be a process within this process, not the entire solution.