BUILDING TRUSTED WHISTLEBLOWING MANAGEMENT SYSTEMS

A PRACTICAL WEBINAR ON STRENGTHENING WHISTLEBLOWING SYSTEMS THROUGH TRUSTED GOVERNANCE FRAMEWORKS.

Andrew Samuels
CEO – WislPort Compliance

Andrew.Samuels@wislportcompliance.com

ISO 37002:2021

A whistleblowing management system

Guidelines for establishing, implementing and maintaining an effective speak-up regime.

THE FOUR-STEP CYCLE

01

Receive

Reports of wrongdoing, through accessible, trusted channels.

02

Assess

Triage, scope, and decide investigative path.

03

Address

Investigate, decide, act, and protect those involved.

04

Conclude

Close cases, communicate outcomes, capture learning.

THREE GUIDING PRINCIPLES

Trust

Reporters trust the system, channels, and people. Without trust, nothing reaches the system.

Impartiality

Reports handled without bias toward reporter or subject; conflicts of interest managed.

Protection

Reporters protected against detriment; confidentiality maintained throughout the process.

Applicable to ALL organizations

Any size · public, private, or not-for-profit · any sector.

Type: Guidelines (Type II) — adoptable, not certifiable. Designed to integrate with existing management systems.

OPERATING MODEL

Plan → Do → Check → Act

The PDCA loop, wrapped by the three principles, anchored in organisational context.

PLAN *Risks, objectives, policy, scope.*	**DO** *Receive · Assess · Address · Conclude.*
ACT	**CHECK**

WHAT EACH STEP ANCHORS

Plan

Risk assessment, policy, scope of system, stakeholder expectations.

Do

The four-step report cycle — Receive, Assess, Address, Conclude.

Check

Monitor outcomes, internal audit, management review — leading indicators matter more than lagging.

Act

Close gaps, capture learning, drive culture improvements.

Intended outcomes *Encourage reporting* · *Protect reporters* · *Resolve reports properly and in time* · *Improve culture and governance* · *Reduce risk of wrongdoing*

ALIGNMENT

One management system. Many regulatory regimes.

ISO 37002 is the bridge between speak-up obligations in law and the operational discipline that delivers them.

ALIGNED WITH (frameworks)

ISO 37301	Compliance Management Systems — 37002 is the speak-up arm of compliance.
ISO 37001	Anti-Bribery (Clause 8.9 reporting concerns) — 37002 operationalises the duty.
ISO 27001	Information security — channel confidentiality and disclosure data protection.
ISO 37301-family	Conduct & ethics standards (37008 investigations, 37002 reporting) work together.
COSO ICIF / ERM	Control Environment, Risk Assessment, Information & Communication components.
IIA Three Lines	Speak-up sits across 1st line (operate), 2nd line (assure), 3rd line (audit).

SUPPORTS (regulation)

EU	Directive 2019/1937 — internal channels mandatory for ≥50-employee orgs across all 27 Member States.
US	SOX §806 + Dodd-Frank §922 — listed-co protections; SEC bounty regime for external disclosures.
UK	Public Interest Disclosure Act 1998 (in ERA 1996) — protected disclosures regime.
SA	Protected Disclosures Act 2000 (as amended 2017) — broad worker-level protection; criminal offence for occupational detriment. Companies Act s.159 + PRECCA s.34 + King IV..
ICC	International Chamber of Commerce Whistleblowing Guidelines — global business-led framework.
OECD/UN	OECD Anti-Bribery Convention Art. 5 · UNCAC Art. 33 — reporting-channel obligations.

Adopt once. Demonstrate against multiple regulatory regimes.

A single 37002-aligned management system is the most efficient route to evidencing speak-up obligations across EU, US, UK, SA, ICC, OECD and UNCAC regimes.

Q1 — TIPS FOR USING THE STANDARD

Five practical tips.

What an organisation establishing a whistleblowing system can actually do with ISO 37002.

01

Be clear on scope.

Define the categories of wrongdoing the system will cover, and who can use it. 37002 covers reports from a broad range of stakeholders — employees, workers, suppliers, contractors, customers. Without explicit scope, the system tries to be everything to everyone and ends up trusted by no one. Write the scope into the policy in plain language; revisit it annually.

02

Earn leadership buy-in — as a business enabler.

37002 is a guideline, not a compliance checkbox. Position it to the board as a risk-intelligence asset: speak-up data is leading indicator on culture, conduct, and operational risk. Without genuine sponsorship, middle management quietly underminees the system. Get the board to name an executive sponsor with skin in the game.

03

Set a positive tone — and use simple language.

Policy and training must use plain language that treats reporters as people doing the right thing, not as suspects. "What you can report" beats "prohibited conduct." "How we protect you" beats "retaliation prohibitions." Training must reach beyond compliance teams — every line manager is part of the system, whether they know it or not.

04

Be proportionate — the right channels for your context.

Not every organisation needs a 24/7 multilingual hotline + an external ombudsman + an anonymous app. Match channels to your size, sector, and risk profile. Critical: ALWAYS provide more than one channel (so the reporter can route around a compromised one), and ALWAYS publish the external escalation path (Public Protector, regulator, etc.).

05

Simple processes — timely handling matters most.

Reporters lose faith fastest when their report disappears into a black hole. Acknowledgement within 7 days. Triage within 30 days. Closure with feedback within statutory windows (90 days under EU 2019/1937 + 3 months under most regimes). Process simplicity beats process completeness — over-engineered workflows are how speak-up systems die.

Anticipating the Pushbacks.

Five questions a sponsor will hear from peers — and the answers that hold up in a board paper.

Q ***"We'll get too many false reports."***

A. Mature systems show ≤ 5% deliberate-malice rate. Training, clear scope, and a triage step filter the rest. False reports are a culture symptom, not a system flaw — and a system that's never tested by a marginal report isn't being trusted by anyone.

Q ***"It will create a culture of snitching."***

A. Evidence shows the opposite. Speak-up culture correlates with HIGHER trust, lower turnover, faster detection of fraud + safety incidents. Most reporters are loyal employees trying to protect the organisation, not punish a colleague. The framing in your policy decides which culture you create.

Q ***"We already have an open-door policy — we don't need this."***

A. Open-door breaks the moment the wrongdoing involves the person whose door it is. A whistleblowing system gives a separate, protected route when the line manager IS the issue, or when the conduct touches the chain of command. The two should coexist; one is not a substitute for the other.

Q ***"Anonymous reports are unreliable — we can't act on them."***

A. ISO 37002 explicitly supports both anonymous and identified channels. Many mature systems show similar substantiation rates between anonymous and named reports. The right framing: anonymity is a SAFETY VALVE for the most fearful reporters; the goal is to make identified reporting safe enough that anonymity isn't needed.

Q ***"This will be weaponised for HR grievances and personal disputes."***

A. Scope discipline (Tip 1) + a proper triage step solve this. Whistleblowing is concerns about WRONGDOING — fraud, safety, regulatory breach, ethical breach. HR grievances run a separate process. Mature triage routes ~30% of inbound reports out of whistleblowing into HR or operations on day one, without losing the reporter's trust.

WHY THIS MATTERS

The benefits — in numbers.

Twenty-plus years of fraud + ethics research, consistent across sources. Whistleblowing systems are the single most effective fraud-detection control we have.

47%
of frauds detected by tips

The #1 detection method — far above internal audit (12%), management review (12%), or external audit (4%).

ACFE Report to the Nations 2024

~50%
lower median loss

When fraud is detected by tip vs. any other method. Earlier detection means less time for the scheme to compound.

ACFE Report to the Nations 2024

33%
faster detection

Organisations with a formal hotline detect fraud schemes substantially faster than those without one.

ACFE Report to the Nations 2024

52%
of tips come from employees

Employees are by far the largest source of fraud tips — they are closest to the wrongdoing and most likely to spot it first.

ACFE Report to the Nations 2024

~42%
substantiation rate

Roughly 4 in 10 reports are substantiated. Anonymous and identified reports substantiate at similar rates.

NAVEX Hotline Benchmark Report

−6.9%
fewer material lawsuits

Peer-reviewed: firms with more internal whistleblowing face fewer lawsuits and lower regulatory fines.

Stubben & Welch, J. Acc. Res. 2020

If you remember one number from this slide: 47%. Tips are the #1 way fraud gets found — and your speak-up system is what turns that into evidence.

SUSA — Speak-Up Self-Assessment

A free online tool to test the quality of your internal speak-up channels, handling systems, and culture-building.

BENCHMARK

ISO 37002

Whistleblowing management systems guidelines

BENCHMARK

EU Directive 2019/1937

EU Whistleblower Protection Directive

BENCHMARK

ICC Guidelines

International Chamber of Commerce

WHAT'S NEW IN THIS VERSION

- Items streamlined for faster completion.
- Scoring against three benchmarks — ISO 37002, ICC Guidelines, EU Directive 2019/1937.
- Improved feedback — see how your organisation compares to averages by sector and size.

FREE TO USE — START NOW

www.susatool.com

For anyone operating or overseeing a speak-up system.

A PARTNERSHIP BETWEEN

EDHEC Business School · Notre Dame Deloitte Center for Ethical Leadership · WislPort Compliance

Andrew Samuels · Jessica McManus Warnell · Mary Gentile