SpeakUp®

Meeting US public company whistleblowing requirements

SOX, exchange listing standards, SEC rules, and DOJ compliance program expectations

For compliance, legal, internal audit, and audit committee stakeholders | August 2026

What this covers

Three questions, answered in order

1 **What US law and guidance actually require**

Ten sources of obligation for a listed company, from the SOX Section 301 mandate through DOJ prosecutorial guidance. Only one is a hard statutory requirement. The statutory requirement. The rest set the practical bar.

2 **Why the standard has risen since 2024**

The DOJ now specifies what a working reporting channel looks like, and two separate 120-day safe harbors put your internal channel on a clock you do not control.

3 **How SpeakUp supports each requirement**

Capability by capability, with every claim traceable to published SpeakUp product documentation, and a clear statement of what we do not do.

SpeakUp®

Part one

The requirement landscape

SpeakUp

Four layers of obligation

Only the first layer is a hard statutory mandate. The other three decide how you are judged

Statutory

- SOX Section 301 and Exchange Act Rule 10A-3
- SOX Section 806 anti-retaliation
- Dodd-Frank Section 21F and Rule 21F-17

Listing and disclosure

- NYSE Listed Company Manual 303A.10
- Nasdaq Listing Rule 5610 and IM-5610
- Item 406 of Regulation S-K

Enforcement guidance

- DOJ Evaluation of Corporate Compliance Programs
- US Sentencing Guidelines Section 8B2.1(b)(5)(C)
- DOJ corporate enforcement and self-disclosure policy, March 10, 2026

Incentive programs

- SEC whistleblower awards, 10 to 30 percent of sanctions
- DOJ Corporate Whistleblower Awards Pilot Program
- Two parallel 120-day internal reporting windows

Only SOX Section 301 tells you that you must have a channel. The other three layers tell you what it has to do, how fast it has to work, and what happens when an employee when an employee decides your channel is not worth using.

SpeakUp

What SOX Section 301 actually requires

Four obligations, owned by the audit committee, not by management

1

Receipt

Procedures to receive complaints regarding accounting, internal accounting controls, and auditing matters.

2

Retention

Procedures to retain those complaints and the record of how they were handled.

3

Treatment

Procedures for how complaints get get reviewed, investigated, and resolved.

4

Anonymous submission

A confidential, anonymous route for for employees raising concerns about about questionable accounting or or auditing.

What the DOJ expects of a reporting channel

The Evaluation of Corporate Compliance Programs is the closest thing to a specification

Works in the right languages

The channel operates in the languages employees employees actually speak.

Uses channels people know

Accessible through the routes employees already use, and widely publicized.

Accepts anonymous reports

Confidential reporting mechanisms are treated as highly probative of real governance.

Handled by qualified people

Investigations are properly scoped, independent, objective, and documented.

Measured on timing

Timing metrics evidence responsiveness, and outcomes are monitored for consistency.

Backed by data and analytics

Compliance has timely access to data and uses it to track program effectiveness.

Source: DOJ Evaluation of Corporate Compliance Programs, revised September 2024

What the DOJ expects after a report lands

Receiving the report is the easy half. Prosecutors spend most of their attention on what comes next

Properly scoped investigations

Handled by qualified, trained people, conducted conducted independently and objectively, and and thoroughly documented.

Root cause analysis

Investigations used to identify root causes, system vulnerabilities, and accountability lapses, not just to close a file.

Consistent discipline

Prosecutors ask directly whether the compliance function monitors its investigations and resulting discipline to ensure consistency.

Real remediation

Concrete changes that reduce the risk of the same issue recurring, tied back to what the root cause analysis found.

Lessons learned

Whether the company reviews and adapts its program based on its own misconduct and that of others facing similar risks.

Measured outcomes

Substantiation rates, average time to complete investigations, and trend analysis across the organization.

Source: DOJ Evaluation of Corporate Compliance Programs

SpeakUp®

Part two

What changed, and why it matters now

SpeakUp®

Your internal channel runs against two clocks

Both regulators give an employee 120 days to report internally first without losing anything

120

days, twice over

The same window appears in both regimes, and it starts the moment your channel receives the report.

SEC, since 2011

Exchange Act Rule 21F-4(b)(7)

An employee who reports internally and then submits the same information to the SEC within 120 days is treated as having reported to the SEC on the earlier internal date. Rule 21F-6 also counts participation in internal compliance as a positive factor in the award, and interference with internal systems as a negative one.

DOJ, since 2025

Corporate Whistleblower Awards Pilot Program

The revised program codified a safe harbor letting a a whistleblower report internally and wait up to 120 days 120 days before contacting DOJ without losing their place their place in line. Under the March 2026 enforcement enforcement policy, the burden of showing you disclosed disclosed promptly sits with the company.

1 Receive

A complete, usable report on first first contact, in the reporter's language.

2 Triage

Severity and routing decided in days, days, not after a manual read of a a backlog.

3 Investigate

Scoped, staffed, and documented, documented, with follow-up questions answered.

4 Decide

Whether to self-disclose, with the the timeliness burden on you.

Sources: 17 CFR 240.21F-4(b)(7) and 21F-6; DOJ Corporate Whistleblower Awards Pilot Program, revised May 12, 2025; DOJ corporate enforcement and self-enforcement and self-disclosure policy, March 10, 2026

The external channel is genuinely competitive

Employees now have a well-publicized, well-funded alternative to your hotline

$60m+

awarded by the SEC to 48 whistleblowers whistleblowers in fiscal year 2025

18

SEC final award orders issued by early July 2026, more than 2.5x all of calendar 2025

30 to 60

submissions a week to the DOJ pilot program portal since it opened

What follows from this

The question is no longer whether employees will report. It is whether they report to you first. A channel people trust, in a language they speak, that answers them back, is what keeps the first report internal.

Sources: SEC Office of the Whistleblower FY2025 Annual Report to Congress; SEC final award orders 2026; DOJ Federal Register notice, May 2026

Part three

How SpeakUp supports each requirement

Reach every employee, in their own language

DOJ expects the channel to work in the languages employees speak, through routes they know

85+

intake languages and regional variants on the default translation model

110+

with the Adaptive AI translation model enabled

60+

languages supported by the Sienna AI voice agent

130+

countries and territories with a SpeakUp phone number, including a US freephone line

How reporters reach you

- Web and app channels, each with their own URL, QR code, and organization code, so you can publicize the route that fits each site or population.
- Phone intake, plus the Sienna AI voice agent, which holds a natural conversation and returns a written record immediately because translation is instant.
- Machine translation by default, human translation on request at additional cost, and the option to read any message in the language the reporter wrote it in.
- Separate channels for third parties, so suppliers, contractors, and partners report through a route you can measure independently of employees.

Source: SpeakUp product documentation, knowledge-base.speakup.com

Anonymous reporting that still lets you investigate

The common failure of anonymous hotlines is a report that arrives incomplete and cannot be pursued

Report without identifying yourself

- Reporters submit through web, app, or phone phone without giving their identity.
- Reporter consent can be enabled or disabled per channel, with your own privacy policy shown at the point of submission.
- Voice files can be enabled or disabled per channel to suit local requirements.

Keep the conversation going

- Case handlers reply to reporter messages and the reporter answers back, so missing detail gets filled in.
- Closing the conversation and closing the issue are separate actions, so the record stays open while the investigation runs.
- Reporters attach documents, and handlers see when they do.

Protect what you no longer need

- AI anonymization clears personally identifiable information across reporter messages and intake form fields while leaving the case context intact.
- Retention is set per field, with Keep, Clear, or AI anonymize applied after the retention period.
- Clear message content, reporter documents, or both from a closed issue when you no longer need them.

An anonymous route satisfies the statute only if it produces something you can act on. A report you cannot follow up leaves your audit committee audit committee with an allegation and no way to treat it, which is the outcome the procedures were written to prevent.

Source: SpeakUp product documentation, knowledge-base.speakup.com

Route around the people a report might implicate

SOX Section 301 puts the audit committee in the chain. Your configuration has to keep it there

Domains	Separate parts of the organization into their own domains, with access granted, changed, or removed at domain level and domains archived when no longer needed.
Roles and permissions	Use pre-defined roles or build custom roles with the exact permissions you want. Administrators are named explicitly.
Issue-level access	Domain access and issue access are distinct. Invite a named user to a single issue, see at any time which users can view it, and change or remove a role on that issue.
Involved parties	Record and manage the parties involved in an issue, and control their access separately from case handlers.
Identity and provisioning	Single sign-on and multi-factor authentication, with SCIM provisioning for automated user and group management.

Source: SpeakUp product documentation, knowledge-base.speakup.com

Evidence that you moved quickly

Timing metrics are what DOJ asks for, and what the 120-day windows make material

Automations

Build rules that fire on a trigger and take an action. action. Set execution priority when several rules rules share a trigger, and write stop rules so conflicting actions do not both run.

Acknowledged on

Every issue carries an acknowledgment date you can view and adjust, so the clock on responsiveness is recorded on the case itself.

Tasks and workflows

Add tasks inside an issue and build custom workflows and issue types, so each category of concern follows the process you designed for it.

Linked issues

Link one issue to another to surface the pattern that a single report would not show.

Reply templates

Standard replies for acknowledgment and feedback, so the first response goes out consistently and fast.

Notifications

Email notifications, customizable per user, so nothing sits unseen in a queue.

Source: SpeakUp product documentation, knowledge-base.speakup.com

Test the channel, do not just install it

DOJ asks whether you periodically test the hotline, for example by tracking a report from start to finish

The two questions prosecutors ask

“Does the company take measures to test whether employees are aware of the hotline and feel comfortable using it?”

“Does the company periodically test the effectiveness of the hotline, for hotline, for example by tracking a report from start to finish?”

What you can do about it

- Send a test issue through any channel and follow it end to end, using the documented procedure.
- Run a setup verification against the documented checklist before you go live and after any change.
- Read the history log on the test case to evidence exactly how long each stage took.

Publicize it to third parties as well, not only employees

DOJ asks how the reporting mechanism is publicized to employees and other third parties. Suppliers, contractors, agents, and business partners see risk your employees never your employees never will. Create a separate channel for them with its own URL, QR code, organization code, branding, and privacy policy, and the reports arrive tagged by reports arrive tagged by channel so you can report on the two populations separately.

Sources: DOJ Evaluation of Corporate Compliance Programs; SpeakUp product documentation

Retain what US law requires, remove what EU law requires

The two regimes pull in opposite directions, and the resolution is configuration, not policy alone

US law says preserve

- Rule 10A-3 requires procedures for the retention retention of complaints, not only their receipt. receipt.
- SOX Section 802 added 18 U.S.C. 1519, which makes knowingly destroying or concealing a record with intent to impede a federal investigation a criminal offense carrying up to 20 years.
- Once litigation or an investigation is reasonably anticipated, preservation obligations attach to the case record.

EU law says minimize

- GDPR storage limitation requires personal data to be kept no longer than necessary for the purpose.
- The EU Whistleblowing Directive and national implementing laws set their own retention limits and confidentiality duties.
- Works councils and data protection officers will ask what happens to reporter data after a case closes.

How you resolve it

- Set retention per field rather than per case, so an accounting complaint and a routine HR concern do not have to follow the same rule.
- Choose Keep, Clear, or AI anonymize for each field after the retention period, so the substance of the case survives while personal data does not.
- Deleting an issue is a permissioned action, and the history log records what happened to the case.

Your counsel sets the retention schedule and decides when preservation overrides it. The platform is what makes the schedule enforceable field by enforceable field by field instead of a policy nobody can operate.

Sources: Exchange Act Rule 10A-3; 18 U.S.C. 1519; GDPR Article 5(1)(e); SpeakUp product documentation

What happens after the finding

Prosecutors ask whether discipline and remediation are consistent. That is a data question

Record the outcome

Close each issue against defined resolution options and record a report outcome, so disposition is a structured field rather than free text in a note.

Connect related cases

Link one issue to another and manage involved parties, so a pattern across sites or a repeat subject becomes visible.

Drive the remediation

Add tasks inside the issue, assign them to named owners, and track them to completion alongside the case itself.

Test for consistency

Build charts on your own resolution and outcome data, filtered by geography, business unit, or seniority, and see whether similar findings produced similar consequences.

Substantiation over time

Track substantiation rates and time to completion by category, which is exactly the effectiveness data the guidance describes.

Feed it back

Export the analysis for the program review that shows you adapted policy, training, or controls in response to what you found.

Source: SpeakUp product documentation, knowledge-base.speakup.com

Produce the evidence, not just the hotline

DOJ expects compliance to have timely access to data and to use it to track effectiveness

Ask questions in plain language

Sienna Insights is an AI chat assistant built into SpeakUp. Ask a question about your about your compliance data and get back a chart, a table, a short summary, or a summary, or a combination.

“Has there been an increase in fraud cases this year?”

“Show me a breakdown of issues by allegation type.”

“Which issues have been open for more than 90 days?”

Sienna only shows data already inside your permission scope, and charts can be saved into your Analytics views for reuse.

Standing reporting for your audit committee

- A dashboard and an issues overview you can filter, reorder, and save as named views.
- Custom charts built on your own case data, downloadable as visual analytics exports.
- Download a single issue as a complete file, or the full issues overview for sampling.
- A history log on every issue, showing what happened to the case and when.
- Date fields documented for behavior, so cycle time reporting holds up under scrutiny.
- SharePoint export and a documented API, webhooks, and app integrations for feeding your own reporting stack.

Source: SpeakUp product documentation, knowledge-base.speakup.com

Requirement to capability map

A single view for questionnaires, audit committee packs, and vendor assessments. One of two

Requirement	What SpeakUp provides	Evidence produced
Anonymous submission (SOX 301)	Web, app, and phone intake without reporter identity, plus the Sienna voice agent	Channel and submission record per case
Receipt and treatment of complaints complaints	Configurable channels, intake forms, issue types, and custom workflows	Case file with full handling record
Audit committee routing	Domains, custom roles, and issue-level access separate from domain domain access	Access list per issue, changeable and viewable
Language and channel access	85+ intake languages by default, 110+ with Adaptive AI, phone numbers in 130+ countries	Language and channel data on every case
Publicized channel	Per-channel URL, QR code, organization code, and custom branding	Channel overview and configuration record
Timing and responsiveness	Automations, acknowledgment dates, tasks, and reply templates	Acknowledged-on and history log per issue
Qualified, consistent handling	Assignment, labels, comments, resolution options, and linked issues	Assignment history and resolution data

Source: SpeakUp product documentation, knowledge-base.speakup.com

Requirement to capability map

Two of two, continuing through testing, retention, analytics, and adjacent disclosures

Requirement	What SpeakUp provides	Evidence produced
Testing the channel	Documented test issue procedure and setup verification checklist	Test case tracked start to finish in the history log
Third-party reporting	Separate channels for suppliers, contractors, and partners	Reporting split by channel and population
Retention and preservation	Retention set per field, permissioned deletion, history log	Retention schedule and record of what was removed removed
Root cause and consistency	Resolution options, report outcomes, linked issues, tasks, and charts	Substantiation and discipline consistency analysis analysis
Data access and analytics	Sienna Insights, custom charts, saved views, exports, API and SharePoint	Dashboards and downloadable analytics
Post-acquisition integration	Case import from legacy systems, new domains, and bulk user import	Migrated case history under one program
Adjacent disclosures (Paths)	Disclosure channels, Employee Hub access, and campaigns	Campaign progress tracking and audit record

Source: SpeakUp product documentation, knowledge-base.speakup.com

SpeakUp

SpeakUp Paths: disclosures and approvals

A separate product, licensed in addition to misconduct reporting, on the same platform

Everything on this slide sits outside the misconduct reporting module. Paths is a distinct product with its own licensing.

1

Disclosure channels

Create channels for disclosure submissions alongside your misconduct reporting channels, with their own settings and their own access rules on the Employee Hub.

2

Issue types and workflows

Build a separate issue type for each category of of disclosure, each with its own custom workflow, workflow, forms, fields, and custom ID format.

3

Campaigns

Run a campaign against a defined population, build build the form employees complete, and track progress as responses come in.

Why it belongs in this conversation

NYSE 303A.10 and Nasdaq 5610 require a code with an enforcement mechanism, and NYSE requires prompt disclosure of code waivers for directors and executive officers. Running disclosures on the same platform as reports means your audit committee sees both in one place, which is where consistency of enforcement becomes something you can evidence.

Source: SpeakUp product documentation, knowledge-base.speakup.com

No platform makes you compliant

Any vendor who tells you otherwise is selling you a risk, not a control

A reporting platform is infrastructure. It carries the channel, holds the record, enforces the routing, and produces the evidence. It does not make the judgments that compliance is actually made of, and a program built on the assumption that it does will fail the first time it is tested.

What SpeakUp provides

- The channel, in the languages and countries your people are in.
- The case record, with routing, access control, retention, and history.
- The workflow that makes your process repeatable across every site.
- The data that lets you show a regulator, an auditor, or your board what the program actually did.

What stays with you

- The legal determination. Whether your program meets your obligations is a conclusion your counsel reaches, not a feature we ship.
- The investigation. We accelerate triage and surface patterns. Your investigators scope the work, weigh the evidence, and make the findings, and they should.
- The culture. No system persuades someone to speak up. It only removes the reasons not to.

Sources

Every claim in this deck traces to a primary source

Legal and regulatory

- SOX Sections 301, 406(c), 802, and 806; Exchange Act Rule 10A-3
- 18 U.S.C. 1519
- Exchange Act Section 21F and Rules 21F-4(b)(7), 21F-6, and 21F-17(a)
- Item 406 of Regulation S-K
- NYSE Listed Company Manual 303A.10; Nasdaq Listing Rule 5610 and IM-5610
- US Sentencing Guidelines Section 8B2.1(b)(5)(C)
- DOJ Evaluation of Corporate Compliance Programs
- DOJ Corporate Whistleblower Awards Pilot Program, revised May 12, 2025
- DOJ corporate enforcement and self-disclosure policy, March 10, 2026
- SEC Office of the Whistleblower, FY2025 Annual Report to Congress

Product

Every product capability described in this deck is published in the SpeakUp knowledge base, which your team can read in full at any time.

knowledge-base.speakup.com

If a claim in this deck is not in our documentation, tell us and we will correct it.

SpeakUp®

Start the conversation

Doing right, made easy.