2026 CCO Playbook

Introduction

Welcome to the 2026 edition of Comply's CCO Playbook, your annual guide to the compliance challenges that matter most, and how to get ahead of them.

If you ended 2025 feeling like you'd finally caught your breath, you weren't imagining it. It was a whirlwind.

A new administration took office with an explicit deregulatory mandate. Paul Atkins was named Chairman of the SEC in April 2025. Fourteen pending SEC rule proposals were formally withdrawn. The off-channel communications sweep, which had generated more than $600 million in penalties across over 70 firms since 2022, concluded formally in January 2025 with nine final actions. After three years of relentless rulemaking velocity, the pace slowed. The slowdown was also structural. A January 20, 2025 White House memorandum ordered agencies to halt new rulemaking until incoming leadership could review and approve pending rules.

For compliance professionals who spent the better part of the last decade running to keep up, the shift was noticeable.

Here is what the data actually showed.

SEC standalone enforcement actions fell to 313 in FY2025. This is the lowest level in a decade, down 27% from 431 in FY2024. Monetary settlements totaled $808 million, the lowest annual total since FY2012[1].

Several rules proposed under Chair Gensler were formally withdrawn, delayed, or still outstanding. These rules are commonly referred to as the Predictive Data Analytics rule, the ESG Disclosure rule, and the Outsourcing Rule, though none carry official titles.

Crypto enforcement was effectively abandoned in favor of a task force approach. The Safeguarding Advisory Client Assets proposal appears unlikely to pass in its current form. The FinCEN AML Rule for RIAs and ERAs, finalized in September 2024, was formally delayed two years via a Federal Register final rule published December 31, 2025[2]. The compliance deadline is now January 1, 2028.

Those are meaningful changes. CCOs are right to register them

But here is what didn't change: examiners still showed up.

Enforcement actions still landed. FINRA's deficiency findings didn't soften. And regulators made their priorities for 2026 unmistakably clear—not through new rules, but through a sharper focus on whether the fundamentals of your existing compliance program actually hold up under pressure.

Chair Atkins' stated focus on investor harm is not a lower bar. It is a different frame.

Where the Gensler era used enforcement to define obligations, the Atkins SEC has signaled it will enforce where harm is clear and firms should have known better. That is cold comfort for any firm whose compliance program has gaps in fiduciary documentation, supervision practices, or marketing review processes. Those gaps are still findable. Examiners are still looking. And the strategies we lay out in this guide will help you prioritize areas of your compliance program that need to be addressed.

The core obligations we all know and love—fiduciary duty, supervision, marketing practices, documentation, client disclosures—are unchanged and under active examination. Chair Atkins has also signaled a focus on personal accountability, and recent enforcement actions serve as a reminder that CCOs themselves can be held responsible when compliance programs fall short.

Layered on top of those unchanged fundamentals is one genuinely new expectation: **Artificial Intelligence (AI) Governance.**

While rulemaking pulled back in some areas, the regulatory expectation around AI moved in the opposite direction. AI has become pervasive across work and life – augmenting how we research, think, write, analyze and synthesize information. Boards and CEOs of organizations of all sizes are looking at AI as a force multiplier for productivity, better decision-making, faster response times, and efficiency gains in areas we've never seen before.

For the first time, both the SEC and FINRA introduced dedicated AI governance sections in their 2026 examination frameworks. Enforcement precedent on AI misrepresentation is already established. The data from Comply's 2026 CCO & Compliance Leader Insights Survey captures the gap precisely: 69% of firms are actively using AI in compliance today. Only 49% have a formal AI policy and governance structure in place. AI is outpacing governance. Regulators noticed.

What's a CCO to do?

The plays in this playbook are built to help you navigate exactly that question – whether you're preparing for an examination, right-sizing your program in a deregulatory environment, or building the AI governance framework your firm hasn't yet documented. This playbook is designed to give you clarity on what matters, what's changed, and what comes next.

Ready to hit play?

> **"It is time for the SEC to end its waywardness and return to its core mission that Congress set for it: investor protection; fair, orderly, and efficient markets; and capital formation."**
>
> SEC Chair Paul S. Atkins, April 22, 2025[3].

SEC & FINRA Enforcement Stats

The headline for 2025 is a decline in the volume of enforcement actions. The story behind it is more instructive than the numbers themselves.

FY2025 was a year defined by transition. A change in SEC leadership, a deliberate recalibration of enforcement priorities, and the most uneven distribution of enforcement activity between an outgoing and incoming administration in over a decade. Understanding what that transition means for your compliance program in 2026 requires more than reading the top-line numbers. It requires understanding what changed, what didn't, and what both regulators are signaling heading into the new year.

SEC Enforcement: A Tale of Two Halves

The SEC brought 313 standalone enforcement actions in FY2025. This is the lowest level in a decade, down 27% from 431 in FY2024 and 38% from 501 in FY2023. Total monetary settlements declined 45% to $808 million, the lowest annual total since FY2012 and less than half of the FY2016–FY2024 average of $1.9 billion[4]. *(Note: The SEC has not published official FY2025 annual enforcement statistics as of the date of this publication.)*

Those numbers tell only part of the story.

Of the 56 enforcement actions brought against public companies and subsidiaries in FY2025, 52 (93%) of the actions were initiated by outgoing Chair Gary Gensler before his departure on January 20, 2025.[4]

The Gensler-era enforcement machine closed out with a record Q1: 200 total actions filed between October and December 2024 the highest first-quarter total in at least two decades. Following the transition in SEC leadership in early 2025, enforcement activity slowed, with relatively few new actions against public companies initiated in the remainder of the fiscal year.

If you're keeping count, this is the fewest in a single year since FY2013.

This is not an enforcement collapse. It's a recalibration—one that shifts focus back to core investor protection principles. For CCOs, the practical question isn't whether the shift is welcome. It's what it means for your program.

Chair Atkins has been explicit: the SEC under his leadership will focus on **"cases of genuine harm and bad acts,"** not on technical books-and-records violations or novel legal theories.

In his October 2025 keynote address, he stated that the off-channel communications sweep, which generated more than $600 million in penalties against over 70 firms during the Gensler years, "consumed excessive Commission resources not commensurate with any measure of investor harm." Nine final off-channel actions were brought in January 2025 as the initiative concluded.[5]

What replaced it was a renewed focus on fraud, insider trading, offering fraud, and fiduciary duty breaches.

Nearly one-third of FY2025 enforcement actions involved offering fraud or insider trading, up from 26% in FY2024. There have also been instances of the SEC closing or dismissing certain high-profile matters, including in areas such as cryptocurrency, cybersecurity, and FCPA enforcement.

What Does This Mean for CCOs?

A lighter enforcement year is not a signal to ease up. The areas the Atkins SEC has deprioritized—technical recordkeeping sweeps, crypto regulation-by-enforcement, novel legal theories—were never the core of most advisory firm's compliance programs anyway. What remains fully active is scrutiny of fiduciary duty, marketing and disclosure accuracy, supervision, and conflicts of interest.

The only SEC risk alert in 2025 was issued on December 16.

And guess what it was about? Marketing Review.

The SEC risk alert flagged continued deficiencies in testimonials, endorsements, and third-party ratings.[6]

FINRA Enforcement: Volume Down, Expectations Steady

FINRA's 2025 enforcement picture mirrors the broader recalibration theme. According to FINRA's official Key Statistics page, FINRA filed 625 new disciplinary actions in 2025, down from 730 in 2024. Fines and disgorgement ordered totaled $99.6 million, with $17.1 million in restitution ordered. FINRA imposed 187 individual bar sanctions and 235 suspension sanctions. (Source: FINRA Key Statistics, finra.org/media-center/statistics)

The directional shift is clear: fewer actions, but higher total monetary penalties compared to 2024's $75.6 million in fines, but context matters.

FINRA's 2025 disciplinary activity remained squarely focused on the same chronic failure patterns that have appeared in every oversight report for the past several years: supervisory system failures, written supervisory procedures (WSPs) deficiencies, books and records breakdowns, AML program gaps, and Reg BI compliance failures. A review of FINRA's monthly disciplinary actions throughout 2025 confirms that these themes drove the overwhelming majority of firm-level sanctions.

The FINRA 2026 Annual Regulatory Oversight Report, published December 2025, illustrated this picture clearly. The same findings that appeared in 2024 and 2023 appear again in 2026—not because regulators have failed to communicate expectations, but because firms have failed to operationalize them.[7]

2026 Regulatory Priorities in the U.S.

2026 SEC Exam Priorities

Within this year's release, the SEC highlighted several specific priorities for investment advisers, investment companies, and broker-dealers, as well as risks likely to impact firms across the industry.

Investment Advisers

ADHERENCE TO FIDUCIARY STANDARDS OF CONDUCT

The Division will focus on investment advice and related disclosures for consistency with fiduciary obligations, including:

- The impact of advisers' financial conflicts of interest on providing impartial advice
- Advisers' consideration of factors associated with investment advice, including cost, investment objectives, characteristics, liquidity, risks, potential benefits, volatility, and likely performance across market conditions
- Advisers seeking best execution to maximize value for clients

Investment products of particular focus include:

- Alternative investments (e.g., private credit and private funds with extended lock-up periods)
- Complex investments (e.g., ETF wrappers on less liquid underlying strategies, option-based ETFs, leveraged and/or inverse ETFs)
- Products with higher costs relative to similar alternatives

Investment recommendations of particular focus include:

- Recommendations to older investors and those saving for retirement
- Advisers to private funds also advising separately managed accounts and/or newly registered funds—reviewing for favoritism in investment allocations and interfund transfers
- Advisers to newly launched private funds
- Advisers that have not previously advised private funds—reviewing for regulatory awareness, liquidity, valuation, fees, disclosures, and differential treatment of investors

Additional adviser types and practices under focus:

- Dually registered advisers where compensation structures may create conflicts of interest
- Advisers utilizing third parties to access client accounts
- Advisers that have merged, consolidated with, or been acquired by existing advisory practices

> **What This Means for 2026:** Fiduciary duty has been a top SEC examination priority for years. It's not going away under the Atkins administration. While the Gensler era pursued technical violations aggressively, the Atkins SEC has said explicitly it will focus on "cases of genuine harm and bad acts."

For CCOs, this means the bar for demonstrating fiduciary compliance has not lowered, it has refocused.

Conflicts of interest, fee disclosures, and the documented rationale behind investment recommendations are exactly the areas where examiners will probe most deeply. If your conflict disclosure practices have not been reviewed since your last exam, now is the time.

EFFECTIVENESS OF ADVISERS' COMPLIANCE PROGRAMS

The Division will focus on whether Policies and Procedures are *reasonably designed* to address conflicts of interest. Areas on which examinations may focus include:

- Whether policies and procedures are implemented and enforced
- Whether disclosures address fee-related conflicts, with focus on conflicts arising from account and product compensation structures
- Advisers with activist engagement practices—accuracy and timeliness of filings on Schedules 13D, 13G, Form 13F, Forms 3, 4, and 5, and Form N-PX
- Compliance practices when advisers change their business models or are new to advising particular asset types, clients, or services

> **What This Means for 2026:** The Division's language here is worth reading carefully: it will assess whether compliance policies are "implemented and enforced," **not just written**. This is the gap that generates deficiency letters.
>
> A compliance program that exists on paper but cannot demonstrate ongoing testing and monitoring is not a compliance program—it is a liability. CCOs should pay particular attention to their annual review process. Examiners will ask for evidence of testing, when it happened, how it happened, and what came out of it—not just attestations that testing occurred. Equally important is what happens after issues are identified: timely remediation is itself an exam focus, and unresolved findings from prior reviews are a red flag.

NEVER-EXAMINED ADVISERS & RECENTLY REGISTERED ADVISERS

As with previous years, the Division will prioritize examinations of advisers that have never been examined, with particular emphasis on recently registered advisers.

> **What This Means for 2026**: If your firm has never been examined or was registered in the past two to three years, move this to the top of your preparation list. The Division has prioritized this category consistently, and that consistency is a signal. First examinations often set the tone for the examiner relationship for years to come. Firms that demonstrate a mature, documented compliance program from day one establishes credibility among the examiners that pay dividends in future cycles.

Investment Companies

Examinations of registered investment companies (RICs) will generally include compliance programs, disclosures, filings, and governance practices.

Areas of particular focus include:

- Fund fees and expenses, and any associated waivers and reimbursements
- Portfolio management practices and disclosures, for consistency with stated investment strategies, fund filings, and marketing materials
- Compliance with the amended fund Names Rule (compliance date extended to June 11, 2026 for larger fund groups; December 11, 2026 for smaller fund groups)
- RICs participating in mergers or similar transactions, including associated operational and compliance challenges
- RICs using complex strategies and/or significant holdings of less liquid or illiquid investments, including valuation and conflicts of interest
- RICs with novel strategies or investments, including funds with leverage vulnerabilities

What This Means for 2026: The Names Rule extension gives fund groups additional runway, but it does not eliminate the obligation to prepare. Examiners will be asking about readiness well before the compliance date. Fund groups that have done nothing to assess their portfolio alignment with fund names since the rule was adopted are behind. If you fall in that group, it's time to get your plan together.

Additionally, the consistency focus, between marketing materials, disclosures, fund filings, and actual practices, mirrors the Marketing Rule scrutiny happening on the adviser side. The standard is the same: what you say must match what you do. Full stop.

Broker-Dealers

FINANCIAL RESPONSIBILITY RULES

- Compliance with the net capital rule and the customer protection rule and related internal processes, procedures, and controls
- Timeliness of financial notifications and other required filings
- Operational resiliency programs, including supervision of third-party and vendor-provided services
- Credit, market, and liquidity risk management controls
- Cash sweep programs and prime brokerage activities, including issues of concentration, liquidity, and counterparty credit risk

What This Means for 2026: Financial responsibility rule failures appeared in FINRA's monthly disciplinary actions throughout 2025 with striking regularity—net capital miscalculations, inaccurate FOCUS reports, reserve account deficiencies. What's interesting is these are not sophisticated compliance failures—they're operational, and with that, avoidable if the right documentation was in place.

Firms with third-party vendors performing financial reporting functions should be asking a direct question: do your Written Supervisory Procedures (WSPs) describe how you supervise that vendor's work—not just that the vendor does the work?

TRADING-RELATED PRACTICES & SERVICES

- Trading practices associated with extended hours trading
- Municipal securities, including rates reset process on variable rate demand obligations, priority of orders, and mark-up disclosure
- Best execution and the pricing and valuation of illiquid instruments
- Order routing and execution information disclosures, including as required by Rule 605 under Regulation NMS
- Regulation SHO—whether broker-dealers are appropriately relying on the bona fide market making exception

What This Means for 2026: Mark-up and mark-down disclosure failures were a consistent FINRA enforcement theme throughout 2025. Multiple firms received six-figure fines for customer confirmation deficiencies that were, at the core, supervisory and WSP failures. Not a technology failure.

If your firm operates in fixed income or municipal securities, a targeted review of confirmation disclosure practices and the supervisory procedures that govern them is a low-cost, high-value exercise before an examiner requests it.

RETAIL SALES PRACTICE, INCLUDING COMPLIANCE WITH REGULATION BEST INTEREST

- Recommendations with regard to products and investment strategies, including account and rollover recommendations

- Conflict identification and mitigation practices, particularly recommendations involving limited product menus
- Processes for reviewing reasonably available alternatives
- Processes for satisfying the Care Obligation, including consideration of customer investment profile and product and account type characteristics

Products of particular focus include:

- Variable and registered index-linked annuities
- ETFs investing in illiquid assets such as private equity or private credit
- Municipal securities, including 529 Plans
- Private placements
- Structured products and alternative investments
- Products with complex fee structures, exotic benchmarks, or illiquid characteristics

> **What This Means for 2026:** Reg BI has been effective since June 2020. Five years in, "we are still building our program" will not satisfy an examiner. The Division's focus on the Care Obligation—specifically how firms document considerations of customer investment profiles against product characteristics—is the area where most deficiencies are found.
>
> This isn't about whether or not representatives are considering what's in the best interest of the client and their investment goals. We hope that is always the case. The question regulators will ask—and you need to provide—is whether your supervisory system generates evidence that they did it. From a regulatory lens, if you can't prove something happened, the examiners cannot confirm that it did. And that's a situation you do not want to be in.

FORM CRS

The Division's examinations will review the content of a broker-dealer's relationship summary, including how the broker-dealer describes:

- The relationships and services it offers to retail investors
- Its fees and costs
- Its conflicts of interest
- Whether the broker-dealer accurately discloses its and its financial professionals' disciplinary history

> **What This Means for 2026:** Form CRS is often a document most firms file and then forget about. But, accuracy, including disciplinary history disclosure, continues to generate findings. Given personnel changes, acquisitions, and new disciplinary history that may have arisen since initial filing, CCOs should build Form CRS accuracy reviews into their compliance calendars as a standing agenda item.
>
> Additionally, the SEC included focus areas for Self-Regulatory Organizations, Clearing Agencies, Municipal Advisors, Transfer Agents, Funding Portals, and Security-Based Swap Dealers.

Industry-Wide Exam Focuses

- **Cybersecurity**—Including AI-related risks and polymorphic malware attacks
- **Regulation S-ID and Regulation S-P** (larger entity compliance deadline: December 3, 2025; smaller entities: June 3, 2026)
- **Emerging Financial Technology**—Including AI representations, AI governance policies, and automated investment tools
- **Anti-Money Laundering**—Program tailoring, independent testing, CIP/CDD, and SAR filing obligations

- **Regulation Systems Compliance and Integrity (SCI)**

What This Means for 2026: The Industry-Wide section contains what may be the most consequential priorities in the entire document for most RIAs and broker-dealers. Reg S-P's incident response program requirement is now in effect for firms with more than $1.5 billion in regulatory assets under management (RAUM). For firms under $1.5 billion in RAUM, the deadline is June 3, 2026.

The Emerging Financial Technology section puts AI governance explicitly in the examination frame. There's a direct mandate to assess whether AI representations are accurate and whether firms have adequate policies to supervise their AI use. This is not a future obligation. It is a present one.

If your firm uses AI in any client-facing or investment-related function, and your compliance program does not address it specifically, that is a gap an examiner will find. And with AI innovations outpacing lawmakers and broader regulatory frameworks, it's safe to assume examiners will be paying extra attention.

All information sourced from the SEC Division of Examinations Fiscal Year 2026

Examination Priorities. For the full document, visit sec.gov/exams.

2026 FINRA Annual Regulatory Oversight Report

Published in December 2025, the 2026 FINRA Annual Regulatory Oversight Report reflects FINRA's commitment to providing member firms with transparency into regulatory observations before examination cycles begin. This year's report is notable for two structural additions: a standalone GenAI section—the first in the report's history—and expanded content on cyber-enabled fraud, senior investor protection, and financial crimes. The FINRA Forward initiative, launched in spring 2025, is threaded throughout, signaling a broader organizational shift toward modernizing rules, empowering member firm compliance programs, and combating emerging cybersecurity and fraud risks.

Financial Crimes Prevention

CYBERSECURITY AND CYBER-ENABLED FRAUD

FINRA identifies a broad and escalating range of cybersecurity threats targeting member firms and their customers, including ransomware and extortion events, data breaches, phishing and smishing attacks, new account fraud, account takeovers, account impersonations, imposter sites, relationship investment scams, and insider threats. Of particular note for 2026, FINRA explicitly calls out Cybercrime-as-a-Service—where criminals with technical expertise sell tools including information stealers, phishing kits, and ransomware to less technical actors—as an active and growing threat to member firms.

> **What This Means for 2026:** FINRA's cybersecurity findings identify GenAI-enabled fraud as an active, escalating threat—including deepfake audio and video, AI-generated imposter sites, false identification documents, and polymorphic malware designed to evade detection. The compliance implication is bidirectional: firms must govern their own AI use and defend against AI being weaponized against their clients and systems. Multi-factor authentication, domain monitoring, outbound email scanning, and third-party vendor risk management are explicitly cited as effective practices—not aspirational ones.

ANTI-MONEY LAUNDERING, FRAUD AND SANCTIONS

FINRA's AML findings in 2026 are extensive and specific. **Key findings include:**

- Failing to reasonably tailor AML programs to the firm's actual business
- Failing to commit sufficient staff and resources to surveillance following material business expansion
- Auto-approving account openings without reasonable customer identity verification; not conducting initial and ongoing risk-based customer due diligence
- Failing to establish policies that can detect identity theft or synthetic identity fraud at account opening

FINRA also flags inadequate due diligence on correspondent accounts of foreign financial institutions and insufficient independent testing of AML programs as recurring findings.

On external fraud, FINRA highlights several escalating schemes impacting investors and member firms:

- Pump-and-dump scams using social media
- Gold bar courier scams

- Crypto confidence frauds
- Mail theft-related check frauds

> **What This Means for 2026:** AML program failures remain among FINRA's most cited findings—specifically the failure to tailor programs to the firm's actual business model, insufficient staffing for surveillance alert review, and inadequate SAR filing practices. These findings have appeared in consecutive oversight reports. Firms still receiving them are not facing a knowledge problem. They are facing an implementation problem. The external fraud findings are a separate but related obligation: firms must build AML programs robust enough to detect not only traditional money movement red flags, but the newer fraud typologies FINRA is now documenting at scale.

MANIPULATIVE TRADING

FINRA continues to focus on manipulative trading activity, including wash trading and prearranged trading, with particular attention to small-cap fraud involving exchange-listed equities with business operations in foreign jurisdictions. In October 2025, FINRA initiated a targeted examination of firm practices in this area.

> **What This Means for 2026**: Firms involved in small-cap underwriting, placement, or trading should review their surveillance parameters and red flag detection processes specifically for the patterns FINRA has identified: nominee accounts, simultaneous trading by seemingly unrelated accounts, and conflicts between the firm and issuer in connection with private capital raises.

GENAI: CONTINUING AND EMERGING TRENDS—NEW FOR 2026

This section appears for the first time as a standalone topic in the report's history. FINRA is explicit that existing rules—supervision, communications, recordkeeping, and fair dealing—apply to the use of GenAI just as they apply to any other technology. Firms evaluating GenAI tools must assess how those tools will comply with applicable regulations, including FINRA Rule 3110 (Supervision), before deployment.

FINRA identifies the top GenAI use case among member firms as "Summarization and Information Extraction"—condensing large volumes of text and extracting entities, relationships, or key information from unstructured documents. Other common use cases include content generation and drafting, workflow automation, conversational AI and question answering, and classification and categorization.

For firms developing or deploying GenAI, FINRA identifies specific considerations across general use, supervision and governance, and emerging agent-based AI systems.

- **On hallucinations and bias**: Firms must assess how models identify and mitigate accuracy risks including misrepresentation of rules, regulations, and policies.
- **On AI agents**: FINRA flags specific risks including autonomy without human validation, scope and authority beyond intended use, auditability and transparency challenges in multi-step reasoning, and data sensitivity risks.

> **What This Means for 2026:** A standalone GenAI chapter in FINRA's oversight report is a structural signal that this topic has cleared the threshold from "emerging" to "examined." Firms that have not yet developed a formal supervisory framework for GenAI—covering development, implementation, monitoring, and documentation—now have clear regulatory expectations to build against. The agent-based AI risks FINRA describes are not hypothetical: they reflect patterns FINRA is already observing at member firms.

Firm Operations

THIRD-PARTY RISK LANDSCAPE

FINRA expects firms to maintain reasonably designed supervisory systems for all outsourced activities. In January 2025, FINRA issued a request for firms to update information related to their third-party vendor engagements, particularly for mission-critical systems. FINRA has since used that information to proactively alert firms of cybersecurity and vendor-related events. Key effective practices include conducting initial and ongoing due diligence on third-party vendors supporting mission-critical systems—specifically including assessment of the third-party vendor's use of GenAI in their products or services—and ensuring contracts prohibit firm or customer sensitive information from being ingested into open-source GenAI tools.

> **What This Means for 2026:** Third-party risk is no longer limited to traditional vendor oversight. The GenAI dimension adds a layer most firms have not yet built into their vendor due diligence frameworks: if your compliance technology vendor is using GenAI in its products, you are responsible for understanding how, and whether your data is protected.

OUTSIDE BUSINESS ACTIVITIES AND PRIVATE SECURITIES TRANSACTIONS

FINRA Rule 3270 and Rule 3280 continue to apply in full. Recurring findings include incorrect interpretation of "selling compensation"—focusing only on direct commissions rather than all direct and indirect financial benefits—and registered persons failing to provide prior written notice of outside business activities (OBAs). FINRA Forward's Regulatory Notice 25-05 proposes a new FINRA Rule 3290 to streamline OBA and PST requirements. As of publication, the filing was pending SEC submission; current requirements remain in effect.

> **What This Means for 2026:** Rule modernization is coming, but it has not arrived. Firms should review their current OBA disclosure and approval frameworks now—both to address existing findings patterns and to position for the requirements that will ultimately follow.

BOOKS AND RECORDS

Recurring findings include failure to retain and archive non-email electronic communications, not establishing adequate procedures for permitted and prohibited communication platforms, and associated persons using personal email or off-channel platforms to communicate with customers without the firm's knowledge. FOCUS report discrepancies resulting from inaccurate net capital and reserve formula computations continue to generate findings.

> **What This Means for 2026:** With the off-channel sweep formally concluded at the SEC level, some firms may be tempted to view recordkeeping as a lower priority. That would be a mistake. FINRA has not signaled any reduction in its own records examination activity, and the underlying obligation—capturing and retaining business-related communications regardless of platform—has not changed.

SENIOR INVESTORS AND TRUSTED CONTACT PERSONS

FINRA findings include firms not making a reasonable attempt to obtain trusted contact person information for all non-institutional customers, failing to provide required written disclosures about TCP, and registered persons attempting to circumvent Rule 3241 by having customers name the registered person's family members as beneficiaries.

MEMBER FIRMS' NEXUS TO CRYPTO

FINRA continues to monitor and respond to crypto-related developments. Key legislative developments include the enactment of the GENIUS Act on July 18, 2025, establishing a regulatory framework for stablecoin issuance. Findings include communications that compare crypto assets to other products without adequate basis, social media communications by influencers that were not fair and balanced, and AML program failures related to suspicious crypto asset transactions.

Communications and Sales

COMMUNICATIONS WITH THE PUBLIC

Findings include inadequate supervision of social media influencers, failure to retain records of influencer communications, inadequate review samples of electronic communications, and failure to review electronic communications in non-English languages where the firm conducts business.

> **What This Means for 2026:** Influencer risk has become a formal examination category. If your firm uses influencers, registered or otherwise, to communicate with the public, your supervisory procedures need to address how that content is reviewed, approved, and retained before it is posted—not after.

REGULATION BEST INTEREST AND FORM CRS

Reg BI findings in 2026 are detailed and specific.

On the Care Obligation:

- Failing to conduct reasonable investigation of offerings prior to recommendation
- Recommending a series of transactions that were excessive in light of customer investment profiles
- Recommending product switches without considering surrender charges, new surrender periods, loss of benefits, and tax consequences

On the Conflict of Interest Obligation:

- Not identifying and disclosing conflicts associated with recommendations

On the Compliance Obligation:

- Writing policies that state the rule requirements but fail to detail how the firm will actually comply

On Form CRS:

- Inaccurately representing disciplinary history with qualifying language
- Omitting or misstating material facts on services offered and cost disclosures
- Incorrectly stating the firm does not provide recommendations
- Failing to deliver Form CRS before or at the time of account opening

> **What This Means for 2026:** Reg BI's Care Obligation failures are increasingly specific—not just "did you consider best interest" but whether your documentation shows how costs and reasonably available alternatives were evaluated for each recommendation. Form CRS failures around disciplinary history are particularly notable: firms that have added disciplinary events since their initial filing and have not updated their Form CRS are sitting on a findable deficiency.

PRIVATE PLACEMENTS

FINRA continues to identify failures in private placement due diligence, including inadequate investigation of the issuer's business, relying solely on past experience with an issuer without fresh diligence, and failure to maintain records evidencing due diligence efforts. FINRA also flags a continuing trend of potentially fraudulent activity in pre-IPO fund offerings, including material misrepresentations about sales compensation and failure to confirm that the fund actually held the pre-IPO shares it purported to have.

ANNUITIES AND SECURITIES PRODUCTS

Variable annuity supervision failures continue to generate disciplinary actions—specifically inadequate suitability documentation for exchanges, insufficient review of existing benefit trades, failure to consider surrender charges and loss of riders, and rates of exchanges that may indicate conduct inconsistent with Rule 2330 or

Reg BI. FINRA also flags that firms should apply heightened policies and procedures to RILA recommendations consistent with the explicit requirements applicable to deferred variable annuities.

Market Integrity

CONSOLIDATED AUDIT TRAIL

Recurring findings include incomplete submission of reportable events, failure to repair errors by the T+3 deadline, and inadequate WSPs for CAT supervisory systems. FINRA also flags unreasonable supervision—specifically not using adequate or varied sample sizes when reviewing CAT reports.

BEST EXECUTION AND ORDER ROUTING DISCLOSURES

Best execution failures include not comparing execution quality in competing markets and inadequate Rule 606 disclosure—particularly incomplete Material Aspects descriptions, inaccurate net payment calculations, and failure to disclose specific terms of payment for order flow arrangements.

> **What This Means for 2026:** Best execution in fixed income and order routing disclosures are a consistent source of FINRA fines. Firms that treat Rule 606 as a back-office filing rather than a supervised compliance output are generating findings that are both avoidable and material.

EXTENDED HOURS TRADING

Extended hours trading receives explicit attention for the first time, reflecting the growth of pre- and post-market retail trading activity. Findings include inadequate supervisory systems for after-hours activity and reporting failures to FINRA's Trade Reporting Facilities.

> **What This Means for 2026:** If your firm has expanded extended hours capabilities, your supervisory procedures need to have kept pace. Extended hours trading is not a niche issue—retail participation in pre- and post-market sessions has grown materially and FINRA is examining for it.

Financial Management

NET CAPITAL

Findings include not recording transactions on an accrual basis, incorrectly classifying or accruing expenses resulting in inaccurate net capital computations, and failing to timely file required notices of net capital deficiencies.

> **What This Means for 2026:** Net capital failures continue to occur at firms of meaningful size—and the common thread is process failure, not intent. WSPs that do not describe how net capital should be calculated, computations performed by a single individual without supervisory review, and FOCUS reports that do not reconcile to general ledger are all findable gaps. Firms that rely on a single FINOP for financial responsibility oversight should assess continuity risk directly.

LIQUIDITY RISK MANAGEMENT AND PROTECTION OF CUSTOMER ASSETS

Customer asset protection and liquidity risk management remain examination areas. Firms should ensure their reserve formula computations are accurate and that customer asset segregation obligations are reflected in current WSPs.

New and Noteworthy

The regulatory road ahead all about orchestrating a well-documented, comprehensive compliance program. It might be tempting to put your compliance program on cruise control.

GenAI Gets Its Own Chapter. For the first time, FINRA's Annual Regulatory Oversight Report dedicated a standalone section to GenAI: Continuing and Emerging Trends – new for 2026. The SEC's FY2026 Exam Priorities include a dedicated Emerging Financial Technology section that explicitly addresses AI representations and AI governance. Both regulators are now examining not just whether firms use AI, but whether they can demonstrate how it is supervised, disclosed, and controlled. This is no longer a future obligation. It is a present examination priority.

Regulation S-P: A Deadline Already Passed for Many Firms. Both regulators identify Reg S-P amendments as an active examination area. Larger entities were required to comply by December 3, 2025. Smaller entities must comply by June 3, 2026. Required elements include written incident response programs designed to detect, respond to, and recover from unauthorized access to customer information—with timely notification to affected individuals.

FINRA Forward. In spring 2025, FINRA launched FINRA Forward—a broad initiative to modernize FINRA rules, empower member firm compliance, and expand cybersecurity and fraud prevention capabilities. Four regulatory notices accompanied the launch: RN 25-04 (rule modernization), RN 25-05 (outside activities), RN 25-06 (capital formation), and RN 25-07 (modern workplace). Rule changes under FINRA Forward may unfold over time—but the signal is clear. Firms should be reviewing their outside business activity frameworks, supervisory procedures, and capital formation practices now, before rulemaking creates new compliance deadlines.

SEC and CFTC Crypto Interpretation: Operative Now. On March 17, 2026, the SEC issued a formal interpretation of how federal securities laws apply to crypto assets, with the CFTC aligning its guidance under the Commodity Exchange Act. This is not proposed or pending, it is in effect. The interpretation establishes a five-category token taxonomy that determines which digital assets are securities and which are not. For CCOs, the immediate obligation is documentation: every digital asset your firm or its employees touch needs to be classified in writing before your next examination. Investment contract analysis is equally urgent—the interpretation explicitly allows investment contracts to terminate, meaning tokens from early offerings may no longer be securities. Trading and pre-clearance policies also need updating to reflect that staking, mining, wrapping, and certain airdrops are now outside securities law. The clock is already running.

The Obligations That Never Went Away

A deregulatory environment creates a specific risk for compliance programs: the temptation to treat silence as permission. When rulemaking activity slows and enforcement headlines fade, firms can begin to deprioritize obligations that never went away. Examiners are trained to spot exactly this pattern.

The following core obligations remain fully in force and are reflected in both the SEC's FY2026 Examination Priorities and FINRA's 2026 Annual Regulatory Oversight Report:

- **Marketing Rule (Rule 206(4)-1):** The SEC issued a second risk alert focused on the Marketing Rule in December 2025. A second risk alert on the same rule is not a coincidence. It is a signal that examiners continue to find that firms are not operationalizing their obligations. Performance advertising, testimonial and endorsement disclosures, and substantiation requirements remain active examination focus areas.
- **Fiduciary Duty:** The Division of Examinations has explicitly prioritized assessments of how advisers identify, disclose, and mitigate conflicts of interest. Fee disclosures, best execution, expense allocation, and compensation arrangements are on the list. Fiduciary duty did not become optional.

- **Regulation Best Interest and Form CRS:** Reg BI has been effective since June 2020. Form CRS since the same date. Five years in, both are expected to be embedded—not still in development. The SEC's 2026 priorities reflect ongoing examination of whether recommendations reflect client-specific best interest analysis and whether Form CRS is accurate and current.
- **Cybersecurity and Reg S-P:** Regulation S-P amendments imposed incident response and notification requirements on registered entities. Larger entities faced a December 3, 2025 compliance deadline—that date has now passed. Smaller entities face a June 3, 2026 deadline. Cybersecurity is among FINRA's top examination priorities for 2026.
- **Supervision and Written Supervisory Procedures:** FINRA noted inadequate WSPs more than 50 times in its 2025 Annual Regulatory Oversight Report. The 2026 report continues to flag supervision as a foundational concern. A WSP that is written but not followed is not a defense.
- **FinCEN AML Rule for RIAs:** Deadline Pushed to 2028.
  - The FinCEN Anti-Money Laundering rule for registered investment advisers and exempt reporting advisers was finalized in September 2024—making it one of the few Gensler-era rules to survive the transition. On December 31, 2025, FinCEN published a final rule in the Federal Register formally delaying the compliance deadline by two years. The new compliance date is January 1, 2028.
  - The delay buys time, but it doesn't change what's coming. When the rule takes effect, RIAs and ERAs will be required to implement full AML and countering the financing of terrorism programs—including a risk-based customer identification program, suspicious activity reporting, and independent testing. A related SEC/FinCEN proposal to extend customer identification program requirements to investment advisers remains pending.
  - CCOs should use the runway wisely. Firms that wait until 2027 to start building their AML programs will face the same implementation crunch that Reg S-P created. The time to gap-assess is now.

Responsible AI Governance, Risk & Compliance Strategies

AI arrived faster than the governance infrastructure built to manage it. That is the defining compliance challenge of 2026—not whether to use AI, but whether the controls, documentation, and supervisory frameworks have kept pace with deployment.

Comply's 2026 CCO & Compliance Leader Insights Survey puts the gap in sharp relief: 69% of firms are actively using AI in compliance today. Only 49% have a formal AI policy and governance structure in place. Nearly half of compliance leaders identify model transparency and explainability as a top concern. That 20-point gap between adoption and governance is not a technology problem. It is an accountability problem—and it sits squarely in the compliance lane.

The regulatory clock is running. The only question is whether your governance framework is running with it.

Understanding AI Technology

Before we get into the regulatory context, let's take a step back. Not every CCO reading this has spent time in the technical weeds of how AI actually works—and the regulatory expectations look very different depending on which type of AI your firm is using.

There are three categories worth understanding, and one characteristic that cuts across all of them.

AI Chat Tools

AI chat tools like ChatGPT, Claude, Gemini, Perplexity are the most familiar. A user types a question or a task, the model responds, and the interaction ends there. The output is only as good as the prompt, and a human reviews and acts on whatever the model produces. But familiarity is where simplicity ends.

Free consumer versions of these tools are not appropriate for firm use. Inputs may be used to train the underlying model, meaning confidential client data, proprietary strategies, or sensitive firm information entered into a free tool has potentially left the building—with no audit trail, no data protection agreement, and no way to retrieve it. The compliance risks are immediate: data security, client confidentiality, and regulatory recordkeeping obligations.

Firms need enterprise-licensed versions with data protection agreements in place, clear policies on what can and cannot be entered, and supervisory procedures governing use. If your employees are using free AI tools on firm business today and your compliance program doesn't address it, that gap is findable.

Custom GPTs and AI-Assisted Workflows

Custom GPTs and AI-assisted workflows are the next layer. These are AI tools built or configured specifically for a firm's use case, like a compliance Q&A tool trained on your policies, a marketing review assistant that flags potential rule violations, or a summarization tool that processes regulatory filings. The model is still responding to prompts, but it has been shaped by the firm's own data, rules, or workflows.

The compliance obligation increases: the firm has made deliberate choices about how the tool is built, what it knows, and how it behaves—and owns responsibility for those choices. That responsibility extends to the compliance team specifically.

When an examiner asks how a custom tool works, how it was built, and what guardrails govern its outputs, "that's a technology question" is not an acceptable answer. The CCO needs to be able to explain it. That requires compliance to be involved in the design and validation process from the beginning—not brought in after deployment to reverse-engineer a governance framework around a tool that's already running.

Agentic AI

Agentic AI is categorically different than the three listed above. An AI agent doesn't just answer—it acts.

It can be given a goal, break that goal into steps, take actions across systems, and iterate toward a result with minimal human input at each stage. Think of an agent that monitors a trading book, flags anomalies, drafts a SAR, routes it for approval, and logs the action—without a human initiating each step.

The efficiency case is obvious. The compliance challenge is equally, if not more, obvious.

How do you supervise something that moves faster than human review? Where do you put the expert-in-the-loop to ensure the outputs are accurate? How do you audit a multi-step reasoning process? Who is responsible when an agent acts outside its intended scope?

These are the questions regulators are asking firms to answer.

Beware of Black Box AI

Black box AI is not a separate type of artificial intelligence—it's a characteristic that can apply to any of the three above, and it's where firms get into serious trouble.

A black box AI is one where the output is visible **but the reasoning behind it is not**. The model produces a result: a recommendation, a risk score, a flagged transaction. But it cannot explain how it got there in terms a human reviewer can interrogate or document.

If an examiner asks how a tool arrived at a particular output and the honest answer is "we don't know," that is a supervision failure by definition. It doesn't matter how accurate the tool has been historically.

You know supervision requires explainability. AI does not change that.

If your firm is using AI embedded in a third-party platform—portfolio analytics, communications surveillance, trade monitoring—and you have never asked whether the underlying model is interpretable, you may have a black box problem you haven't identified yet. That is vendor oversight risk and supervisory risk at the same time.

Understanding these distinctions matters because the regulatory expectations are not uniform across all four. The compliance infrastructure required to govern an AI chat tool is meaningfully different from what is required to govern an AI agent—and both are different from what is required when the AI making decisions cannot explain itself.

Who Owns AI Governance?

The governance gap regulators are describing is not fundamentally a technology problem. It is an organizational accountability problem. The question "who owns AI governance?" is one most firms have not answered cleanly. The ambiguity has consequences. When ownership is unclear, governance doesn't happen. When governance doesn't happen, firms deploy tools they cannot explain to an examiner.

The compliance answer is direct: the CCO cannot own implementation, but the CCO must own the supervisory framework. That means partnering with technology, legal, and business leadership to:

- Define what the firm's AI use cases are
- Establishing criteria by which new tools get evaluated and approved
- Design the testing and monitoring procedures that apply once tools are deployed
- Ensure client-facing representations about AI are accurate and current

Compliance is not the technology team. But compliance is the function with the regulatory fluency to define what "governed" means in practice. It's up to you to enforce it enforce it.

According to Comply's 2026 survey, **41% of compliance leaders identify AI usage and governance as an internal education gap.** That figure reflects an organizational reality most CCOs know firsthand. The people building and deploying AI tools often don't know what the compliance obligations are, and the compliance team often doesn't have enough technical context to ask the right questions. Closing that gap is not a training exercise. It is a cross-functional governance challenge that requires compliance expertise at the table when AI decisions are being made—not after.

The CCOs who navigate this best in 2026 will not be the ones with the most sophisticated AI tools. They will be the ones who can show an examiner what AI is being used, how it was evaluated, how it is supervised, and how what they have told clients about it matches reality. The combination of technical awareness, documented controls, and human accountability is what defensible AI governance looks like—and we're here to help.

What Examiners Will Ask For

The SEC and FINRA are not asking whether your firm uses AI. They are asking whether you can demonstrate that your use of AI is supervised, disclosed, and controlled—and whether a human with the right expertise is accountable for the outputs it produces. In practice, that means an examiner will want to see evidence across five areas.

- **An AI Inventory.** What AI tools are being used across your firm, in what functions, and who approved them? This includes AI embedded in third-party platforms, not just purpose-built AI products. Firms that cannot produce a current, accurate inventory of where AI operates in their business cannot credibly claim to be supervising it. An inventory is the foundation—the prerequisite for every governance step that follows.
- **AI Governance and Approval Process.** How does a new AI tool get evaluated before deployment? What criteria govern the decision? Who signs off, and what gets documented? FINRA is explicit: firms evaluating GenAI tools must assess how those tools will comply with applicable regulations, including FINRA Rule 3110 (Supervision), before deployment.

The "we tried it and it seemed fine" is not a governance process. A documented approval workflow, with defined criteria, compliance involvement, and accountable reviewers, is. Critically, compliance expertise must be part of that evaluation—not a downstream review after the tool is already embedded in the workflow. Effective AI governance requires cross-functional input: compliance, risk, technology, and senior leadership all need a seat at the table. A process owned by one function alone is not a governance process.

- **Supervision and Testing Documentation.** How is the tool's output reviewed once it's in production? What validation steps are in place to catch hallucinations, bias, or accuracy degradation over time? FINRA specifically calls out the need to assess how models identify and mitigate accuracy risks—including misrepresentation of rules, regulations, and firm policies. For AI used in client-facing or investment-related functions, the supervisory bar is higher: if the tool informs a recommendation, the firm bears supervisory responsibility for what it produces. Human review is not optional. It is the control.
- **Disclosure and Representation Review.** Have you reviewed your client disclosures, Form ADV, and marketing materials for AI-related representations? AI claims must be accurate, substantiated, and aligned with what your systems actually do. If you make a claim about AI in your marketing or your Form ADV, that claim must be verifiable. Firms that have not reviewed their disclosures since deploying new AI tools are carrying an enforcement risk they may not know they have.
- **Vendor Oversight That Includes AI.** If your compliance technology vendor, portfolio analytics platform, or communication surveillance tool uses AI in its products or services—you are responsible for understanding how. FINRA explicitly calls out that firms must assess their vendors' use of GenAI and ensure that contracts prohibit sensitive firm or customer data from being ingested into open-source AI tools. Third-party AI risk is not a vendor's problem to manage. It is yours to supervise.

The AI Agent Problem—and Why It Requires a Different Supervision Model

AI agents represent a qualitatively different compliance challenge from other AI tools—not just a more complex version of the same problem. The supervision model that works for a prompt-based AI tool does not translate to an agent that takes autonomous, multi-step action across systems. FINRA's 2026 report describes patterns already observed at member firms, not hypothetical risks. They deserve direct attention.

The specific risks FINRA identifies are:

- **Autonomy without human validation**—agents acting without requiring approval at each step
- **Scope and authority beyond intended use**—agents performing actions outside their defined parameters
- **Auditability challenges**—multi-step reasoning that is difficult to reconstruct or explain after the fact
- **Data sensitivity**—agents accessing or transmitting information beyond what the task requires

Each maps directly to a supervisory obligation. Autonomy without human validation is a supervision gap. Scope creep is a control failure. Auditability gaps mean you cannot demonstrate compliance after the fact. Data sensitivity issues are potential confidentiality and recordkeeping violations.

The 2026 Compliance Plays

Every playbook needs plays. What follows are eight practical moves compliance leaders at investment advisers and broker-dealers can make right now—to get ahead of examiner expectations, close the gaps that generate deficiency letters, and build programs that scale. None of these are theoretical. Each are grounded in what the SEC, FINRA, and the data are telling us about where firms are falling short in 2026.

1. Establish an AI Governance Framework

The goal is not a perfect AI governance program on day one. The goal is a defensible one. A program that demonstrates your firm has thought seriously about the obligation, put structure around it, and is actively managing it. Here is a practical starting point.

- **Conduct an AI inventory.** Know what is deployed, where, and who approved it. If you don't have this, nothing else is possible. Include AI embedded in third-party platforms, not just standalone tools.
- **Document your approval process.** Even a simple framework including what criteria must be included in an evaluation and who within compliance and IT needs to review, document, and approve it, is meaningfully better than no process at all. Compliance must be part of that approval chain.
- **Review your disclosures.** Does what you have told clients and regulators about your use of AI match what you are actually doing? This is the most direct enforcement risk, and it is the easiest one to close.
- **Extend your vendor due diligence.** Add AI-specific questions to your vendor assessment process. If a vendor uses AI in its products, you need to know how, what data it touches, and whether the outputs are interpretable.
- **Build the expert-in-the loop supervisory framework.** Define how AI output gets reviewed, what triggers escalation, and how that review is documented. A governance policy that lives in a document and never intersects with a real workflow is not a control. It is a liability.
- **Invest in AI training and education.** The 41% of firms identifying AI governance as an internal education gap are describing a solvable problem.[8] Compliance teams that understand how their firm's AI tools work—not at an engineering level, but at a functional level—are better positioned to govern them, better positioned to explain them to an examiner, and better positioned to catch problems before they become findings.

2. Get Your Marketing House in Order

The SEC issued a second risk alert focused on the Marketing Rule in December 2025. A second alert on the same rule is not a coincidence. It is a signal examiners are still finding the same deficiencies—and firms have not operationalized their obligations even after multiple rounds of regulatory guidance.

For investment advisers, the Marketing Rule (Rule 206(4)-1) governs how performance is advertised, how testimonials and endorsements are disclosed, and how third-party ratings are used. The second risk alert flagged continued deficiencies in all three areas. For broker-dealers, FINRA Rule 2210 governs communications with the public—and the 2026 oversight report flags inadequate supervision of social media influencers, failure to retain records of influencer communications, and inadequate review of electronic communications as recurring findings across both firm types.

For both investment advisers and broker-dealers, the marketing review process should include:

- A documented pre-publication review workflow with defined approval criteria and a clear audit trail
- A substantiation file for any performance claims, testimonials, endorsements, or third-party ratings used in advertising
- A social media and influencer policy that addresses how content is reviewed, approved, and retained before it is posted
- A periodic review of existing marketing materials—not just new ones—for continued accuracy and compliance
- An assessment of whether AI-generated marketing content has been reviewed under the same standards as human-drafted materials

If your marketing review process relies on a single reviewer with no documented criteria and no retention system, that is not a process. It is a single point of failure.

3. Your Form ADV and Form CRS for Accuracy

Form ADV and Form CRS are living documents. Most firms treat them as annual filings. Examiners treat them as representations—and they read them before they walk in the door.

For investment advisers, Form ADV Part 2 is the foundational disclosure document. For broker-dealers, Form CRS is the relationship summary that retail investors receive at account opening. Both are active examination targets in 2026. The FINRA 2026 oversight report specifically flags inaccurate disciplinary history disclosures on Form CRS—including firms that added qualifying language to explain away disciplinary events—as a finding category. The SEC's exam priorities flag fee disclosures, conflict descriptions, and consistency between what is disclosed and what is actually practiced. The SEC has also become increasingly sophisticated in using technology to cross-reference filings—flagging inconsistencies between Form ADV, Form PF, and marketing materials at scale. Firms should be applying the same discipline, using technology to audit their own disclosures for consistency before an examiner does it for them.

An accuracy audit should cover:

- **Disciplinary History:** Has anything changed since your last filing that requires disclosure or update?
- **Fee Structures:** Do your current compensation arrangements match what is described in Part 2A or Form CRS?
- **Conflicts of Interest:** Are all material conflicts identified, and are your mitigation practices described accurately?
- **AI Representations:** If your Form ADV or marketing materials make any claim about your use of AI, does that claim match what your systems actually do?
- **Services Offered:** For broker-dealers, does Form CRS accurately describe the services you provide to retail investors and any limitations on those services?

Form ADV annual updates are due within 90 days of your fiscal year-end. For most December 31 fiscal year firms, that is March 31. Do not treat it as a filing exercise. Treat it as a disclosure accuracy review.

4. Run a Risk Assessment to Inform Your Policies and Procedures Review

A policies and procedures review without a risk assessment behind it is an editing exercise. It may produce cleaner documents. It will not produce a more effective compliance program.

The right sequence is risk assessment first, policy review second. The risk assessment identifies where your firm's actual activities, business model, and personnel create compliance exposure. The policy review then addresses whether your current documentation adequately governs those specific risks. For investment advisers, this means assessing exposure under the Advisers Act—fiduciary duty, conflicts, marketing, custody. For broker-dealers, it means assessing exposure under FINRA's rulebook—supervision, Reg BI, books and records, AML. For dual registrants, it means doing both.

A well-constructed risk assessment for 2026 should specifically address:

- Where AI is being used in your firm and whether your policies govern it
- Whether your marketing review procedures reflect the current Marketing Rule requirements and the second risk alert's findings
- Whether your P&Ps , WSPs, AML manuals and other compliance documents have kept pace with changes in your business, personnel, and technology
- Whether third-party and vendor relationships are covered by your policies, including AI-specific vendor risk
- Whether your incident response procedures satisfy the Reg S-P requirements that are now in effect for larger entities and coming for smaller ones

The annual risk assessment is also the document that drives your compliance calendar, your testing priorities, and your annual review agenda.

5. Assess Your Third-Party, Vendor, and Cybersecurity Risk

Third-party risk management has always been a compliance obligation. In 2026, it has a new dimension: almost every significant vendor your firm relies on has incorporated AI into its products—and most firms have not updated their vendor oversight frameworks to account for it.

For investment advisers, the Advisers Act requires that compliance policies and procedures address vendor relationships that are material to the firm's operations. For broker-dealers, FINRA Rule 3110 requires supervision of outsourced functions. For both, the Reg S-P amendments impose specific requirements around incident response and the protection of customer information—including information held by third-party service providers. Larger entities were required to comply by December 3, 2025. Smaller entities face a June 3, 2026 deadline.

A comprehensive third-party and cybersecurity review for 2026 should address:

- Whether your vendor contracts include data protection provisions that specifically address AI—prohibiting sensitive firm or customer data from being ingested into open-source models
- Whether you have conducted due diligence on your vendors' AI use, and whether that diligence is documented
- Whether your incident response program is written, tested, and meets the Reg S-P requirements applicable to your firm size
- Whether your P&Ps and/or WSPs describe how you supervise outsourced functions—not just that a vendor performs the function
- Whether your cybersecurity program addresses the specific threats FINRA has flagged for 2026: ransomware, phishing, account takeovers, deepfake-enabled fraud, and Cybercrime-as-a-Service

The firms that treat third-party risk as a contract review exercise rather than an ongoing supervisory obligation are generating findings. The firms that treat cybersecurity as an IT responsibility, rather than a compliance one, are carrying Reg S-P exposure they may not have identified.

6. Prepare for Your Next Examination

Examination preparation is not a sprint you run when you receive the document request list. It is a program posture you maintain year-round. CCOs that perform best in examinations are not the ones that feel ready. They're the ones that can prove it.

One best practice that separates prepared firms from reactive ones: a Day 1 presentation. When examiners arrive, having a concise, well-organized overview of your business—your model, your clients, your key personnel, your compliance program structure—gives you control of the narrative from the start. It demonstrates maturity, builds credibility with the examination team, and reduces the likelihood that examiners fill in gaps with their own assumptions. Firms that wait to be asked are already behind.

The Atkins-era examiner is not going away. What has changed is the frame. Where the Gensler era pursued technical violations aggressively, the Atkins SEC has stated it will focus on genuine harm and bad acts. For investment advisers, fiduciary failures, undisclosed conflicts, and marketing misrepresentations are squarely in scope. For broker-dealers, it means Reg BI Care Obligation failures, Form CRS deficiencies, and supervisory system breakdowns are the primary targets. FINRA has not signaled any reduction in examination intensity—the same chronic failure patterns that drove 2025 disciplinary actions will drive 2026 ones.

Exam readiness for 2026 means being able to demonstrate the following on short notice:

- Your compliance manuals are current, reflect your actual business, and show evidence of testing
- Your annual review was conducted, documented, and produced follow-up action items that were tracked to completion
- Your marketing materials were reviewed, approved, and retained in accordance with applicable rules
- Your conflict of interest disclosures in Form ADV or Form CRS are accurate and current
- Your AI governance framework—including the inventory, approval process, supervisory loop – is documented and demonstrable
- Your Reg S-P incident response program is in place (for firms with more than $1.5 billion in RAUM) or on a documented implementation timeline (for firms with less than $1.5 billion in RAUM, the deadline June 3, 2026)

Never examined firms and recently registered advisers should move this to the top of the list. The Division of Examinations has consistently prioritized this category, and the first examination often sets the tone for the examiner relationship for years.

7. Build Your Annual Review into a Strategic Asset

The annual review is the most consistently underutilized tool in the compliance program. For investment advisers, Rule 206(4)-7 requires it. For broker-dealers, FINRA Rule 3120 requires an annual report on the supervisory control system. Most firms complete the obligation. Fewer use it strategically.

The difference between a compliance program that improves year over year and one that circles the same findings is almost always the quality of the annual review. A review that asks "did we do what we were supposed to do?" produces attestations. A review that asks "where is our program actually exposed?" produces a roadmap. The SEC's exam priorities say explicitly that examiners will assess whether compliance policies are implemented and enforced—not just written. The annual review is your primary evidence that they are.

For 2026, a strategic annual review should:

- Be driven by your risk assessment—test the highest-risk areas of your program, not just the easiest ones to document

- Produce specific findings with owners and deadlines, not just a summary conclusion
- Include a dedicated section on AI governance—inventory current, policies documented, supervisory loop functioning
- Address any changes in the firm's business, personnel, or technology since the last review
- Generate a written report that can be produced to an examiner, with evidence of follow-up on prior year findings

The CCO who presents the annual review to the board or senior management as a strategic program assessment—rather than a compliance checkbox—is the CCO who earns the organizational standing to ask for resources. That is not a governance nicety. It is a program management imperative.

8. Invest in Compliance Education

The compliance professional who stopped learning when the rulemaking slowed is already behind. The 2026 compliance environment rewards expertise—in the examination room, in the boardroom, and in the increasingly complex technology decisions that now land in the compliance lane.

For compliance teams at investment advisers and broker-dealers, the education gap is specific and addressable. Comply's 2026 survey identified AI governance as the top internal education gap—**41% of compliance leaders said their teams are not sufficiently equipped to govern AI use at their firms.** That is a solvable problem, and it starts with leadership modeling the behavior. If the CCO is not conversant in how AI tools work, what the regulatory expectations are, and how to evaluate a vendor's AI claims, it is unrealistic to expect the rest of the team to be.

A compliance education strategy for 2026 should include:

- **AI literacy for compliance staff**—not engineering-level depth, but enough functional understanding to govern, evaluate, and explain the tools the firm uses
- **Regulatory update cadence**—a structured process for tracking SEC risk alerts, FINRA regulatory notices, exam priority publications, and enforcement actions, and translating them into program implications
- **Role-specific training for registered representatives and investment adviser representatives** on Reg BI, fiduciary duty, marketing standards, and supervision obligations
- **CCO peer networking and engagement** at industry conferences, roundtables, and networks where compliance leaders share what they are seeing in examinations and regulatory interactions
- **Documentation of training completion** for both regulatory evidence purposes and to demonstrate to examiners that the firm takes ongoing education seriously

The compliance function that invests in education is not spending money on training. It is building the institutional knowledge that makes everything else in this playbook possible.

Conclusion

The 2026 compliance landscape is not defined by what regulators have pulled back—it is defined by what they haven't. Fiduciary duty, supervision, marketing accuracy, cybersecurity, and client disclosures remain as examined today as they were under the most active rulemaking environments of the past decade.

The Atkins-era shift in enforcement philosophy does not lower the bar for compliance programs, it refocuses attention on the fundamentals that have always mattered most. Firms that treat a quieter rulemaking calendar as an invitation to ease up on their programs will find examiners arriving with the same expectations—and finding the same gaps—that generated deficiency letters in prior years.

The CCOs who navigate 2026 successfully will be those who use this moment of relative stability not to pause, but to strengthen the foundations of their programs: documented controls, tested policies, accurate disclosures, and a supervisory framework that can stand up to scrutiny.

The other defining challenge of 2026 is one that has no historical parallel. The obligation to govern AI in real time, without settled rules, as the technology evolves faster than the frameworks meant to manage it. That challenge requires something no regulation can prescribe—judgment.

The compliance plays in this guide are not a formula. They are a starting point for building programs that are defensible, adaptive, and grounded in what regulators are actually asking for. Whether you are preparing for a first examination, right-sizing your program in a deregulatory environment, or building AI governance infrastructure from scratch, the path forward is the same: know your risks, document your controls, and close the gap between what you have told regulators and clients you do, and what you can actually prove you are doing.

If you need help building and scaling your compliance program, Let's talk.