SAI360
CONNECTED ETHICS RISK & COMPLIANCE

The CCO Playbook

A Strategic 90-Day Operational Guide & Executive Readiness Guide

Executive Summary

Stepping into the role of Chief Compliance Officer (CCO) represents a fundamental shift in executive accountability. Beyond legal interpretation and retrospective policy drafting, the modern CCO assumes operational ownership of organizational governance and regulatory integrity. To establish an authoritative and resilient compliance posture, newly appointed CCOs must transition from passive risk oversight to an active, evidence-based Governance, Risk, and Compliance (GRC) operational strategy.

This operational playbook provides a structured implementation methodology, comparative framework evaluation, and a phase-by-phase execution checklist designed for executive transitions during the first 90 days.

Core Compliance Framework Evaluation Matrix

Aligning organizational operations with established regulatory frameworks provides a defensible methodology and standardizes reporting structures for the Board of Directors.

Framework	Authoritative Body	Core Pillars & Criteria	Primary Application Context
DOJ ECCP	U.S. Department of Justice	Program design adequacy, resource sufficiency, operational empowerment, and practical effectiveness testing.	Entities subject to U.S. federal jurisdiction and cross-border regulatory enforcement.
ISO 37301	International Organization for Standardization	Compliance Management System (CMS) requirements, continuous risk evaluation, leadership accountability, and structural governance.	Global enterprises require accredited, certifiable standards for international commercial partners.
OIG Guidelines	HHS Office of Inspector General	Seven core elements: written standards, compliance leadership, education, effective communication channels, auditing, disciplinary enforcement, and immediate corrective action.	Healthcare providers, health systems, payors, pharmaceutical manufacturers, and life sciences organizations.
SEC / FCPA Guidance	SEC & DOJ	Anti-bribery provisions, internal accounting controls, third-party intermediary vetting, and hospitality governance.	Publicly traded entities and organizations executing transactions within foreign jurisdictions.

Industry Regulatory Mapping & Control Architecture

An effective compliance structure maps global policy standards to specific statutory and regulatory mandates relevant to the operating environment.

1. Healthcare Compliance & Regulatory Governance

- **Statutory Mandates:** Health Insurance Portability and Accountability Act (HIPAA), HITECH Act, Anti-Kickback Statute (AKS), Physician Self-Referral Law (Stark Law), and the False Claims Act (FCA).
- **Control Requirements:** Protected Health Information (PHI) encryption, medical director agreement auditing, provider exclusion screening, fair market value (FMV) verification, and billing audit protocols.

2. Corporate Ethics, Anti-Corruption & Whistleblower Oversight

- **Statutory Mandates:** Foreign Corrupt Practices Act (FCPA), UK Bribery Act, French Sapin II Law, and Sarbanes-Oxley Act (SOX) Section 806.
- **Control Requirements:** Third-party intermediary due diligence, gift and entertainment declaration workflows, anonymous reporting channels, and anti-retaliation enforcement mechanisms.

3. Data Governance, Privacy & Operational Resilience

- **Statutory Mandates:** General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA/CPRA), EU Artificial Intelligence Act, and cross-border transfer framework regulations.
- **Control Requirements:** Data inventory mapping, automated privacy impact assessments (PIA), vendor risk categorization, and incident response notification protocols.

The 90-Day Phased Implementation Playbook

This structured milestone playbook outlines the strategic objectives, key activities, and required deliverables across the first three months of tenure.

90-DAY STRATEGIC IMPLEMENTATION TIMELINE

[Days 1 - 30]	[Days 31 - 60]	[Days 61 - 90]
Discovery & Culture Baseline	Gap Analysis & Risk Appetite	Operationalization & Board Reporting

Phase 1: Days 1 to 30 — Discovery, Stakeholder Diagnostic & Baseline Assessment

STRATEGIC OBJECTIVES

- Analyze informal communication pathways and operational compliance friction.
- Construct an exhaustive regulatory obligation inventory and map existing governance assets.

EXECUTION TASKS

1. Executive Stakeholder Inquiries: Conduct structured diagnostic interviews across business units, including operations, legal, human resources, internal audit, information security, and finance.

2. Obligation Mapping: Catalog all international, federal, state, and industry-specific regulatory obligations governing current and planned business operations.

3. Culture Baseline Survey: Deploy an anonymous, organization-wide survey measuring employee perception of organizational ethics, psychological safety, and confidence in reporting channels.

4. Third-Party Ecosystem Inventory: Compile a centralized registry of active vendors, distributors, sales agents, and high-risk third-party intermediaries.

5. Retrospective File Review: Audit historical litigation, internal investigation logs, regulatory inquiries, and previous internal/external audit findings.

PHASE 1 DELIVERABLES

- Comprehensive Regulatory Obligation Matrix
- Key Stakeholder Diagnostic Summary
- High-Risk Third-Party Intermediary Inventory
- Quantitative Compliance Culture Baseline Report

Phase 2: Days 31 to 60 — Gap Analysis, Risk Appetite Alignment & Governance Modernization

STRATEGIC OBJECTIVES

- Evaluate current operational controls against DOJ ECCP and ISO 37301 standards.
- Formalize the institutional compliance risk appetite and update core governance policies.

EXECUTION TASKS

1. Control Gap Analysis: Conduct a comparative audit of existing controls against target regulatory framework criteria to identify coverage gaps.

2. Risk Appetite Formalization: Facilitate executive leadership workshops to define quantitative and qualitative risk thresholds across strategic categories.

3. Enterprise Compliance Risk Register: Construct a weighted risk register evaluating potential compliance failures by likelihood, inherent severity, and residual risk score.

4. Policy Governance Review: Review and update essential governance policies, including the Code of Conduct, Whistleblower Policy, and Conflicts of Interest Policy.

5. Strategic Remediation Roadmap: Formulate a prioritized action plan targeting the top 10 identified compliance vulnerabilities for executive sign-off.

PHASE 2 DELIVERABLES

- Formal Compliance Gap Analysis Report
- Weighted Enterprise Compliance Risk Register
- Modernized Code of Conduct & Governance Policy Suite
- Executive Priority Remediation Plan

Phase 3: Days 61 to 90 — Operationalization, Workflow Automation & Executive Scorecards

With the rapid proliferation of Generative AI tools and automated decision engines, organizations face new vectors of operational risk. AI governance can no longer operate in a technology silo; it must be embedded directly into core Enterprise Risk Management (ERM) programs.

STRATEGIC OBJECTIVES

- Transition compliance administration from manual processes to automated, scalable digital workflows.
- Implement outcome-oriented compliance metrics and present an executive scorecard to the Board of Directors.

EXECUTION TASKS

1. System Centralization: Migrate policy distribution, employee attestations, and conflict disclosures to an integrated digital management system.

2. Hotline & Triage Optimization: Standardize intake protocols, investigation Service Level Agreements (SLAs), and executive escalation paths for internal reports.

3. Role-Based Training Deployment: Roll out specialized, scenario-based training modules tailored to high-risk roles and middle managers.

4. Automated TPRM Cadence: Implement automated risk scoring, screening, and periodic re-evaluation for third-party partners.

5. Board Scorecard Finalization: Establish executive dashboard metrics tracking program health, training completion, investigation timelines, and open risk remediation.

PHASE 3 DELIVERABLES

- Executive Board Compliance Scorecard
- Automated Policy Attestation Infrastructure
- Automated Third-Party Risk Management Protocol
- Whistleblower & Incident Tracking Dashboard

Whistleblower Hotline Triage & Escalation Architecture

Establishing clear triage protocols ensures critical disclosures are investigated promptly and reported appropriately.

Severity Tier	Qualification Examples	Target Investigation SLA	Recommended Escalation Pathway
Tier 1: Critical	Executive misconduct, systemic accounting fraud, bribery/FCPA violations, severe health and safety risks.	Immediate intake (< 24 hours); Investigation within 7 days	Chief Executive Officer, Audit Committee, Board of Directors
Tier 2: High	Middle management conflict of interest, localized billing irregularities, significant data privacy breaches.	Intake within 48 hours; Investigation within 14 days	CCO, General Counsel, Relevant Business Unit Head
Tier 3: Moderate	Isolated policy non-compliance, vendor policy deviations, localized workplace disputes.	Intake within 72 hours; Investigation within 30 days	Compliance Director, Human Resources Leadership

Executive Board Reporting Scorecard Template

To demonstrate structural effectiveness to executive leadership and the Board of Directors, focus on outcome-based key performance indicators (KPIs) rather than volume-based metrics.

Performance Category	Key Performance Indicator (KPI)	Target Benchmark	Reporting Cadence
Culture & Awareness	Policy attestation rate for high-risk personnel	100% within 30 days	Quarterly
Program Responsiveness	Mean time to initiate inquiry following hotline report	< 48 hours	Monthly
Investigation Efficiency	Average days to conclude internal investigation	< 30 business days	Quarterly
Third-Party Risk	High-risk vendors completing due diligence prior to engagement	100% compliance rate	Bi-Monthly
Remediation Tracking	Audit and investigation recommendations implemented on schedule	> 95% compliance rate	Quarterly

Architectural Transition: Spreadsheet Vulnerabilities vs. Integrated GRC Architecture

Relying on disconnected spreadsheets for risk tracking, policy management, and vendor oversight introduces significant operational friction and audit risk.

Functional Area	Spreadsheet-Based Management	Integrated GRC System of Record
Audit Evidence Verification	High risk of file corruption, version discrepancies, and unverified edits.	Automated immutable audit logs with cryptographic timestamping.
Policy Attestation	Manual email distribution with unverified tracking mechanisms.	Automated delivery, comprehension testing, and real-time attestation tracking.
Conflict of Interest (COI) Tracking	Fragmented form collection via individual email inbox folders.	Centralized digital disclosure portals with automated manager review routing.
Board Reporting	Manual slide compilation subject to human error and data latency.	Live analytics dashboards generating real-time executive reports.

Regulatory Examination & Enforcement Readiness

A new CCO must be prepared to respond to regulatory examinations, government inquiries, and enforcement actions from the outset. Proactive readiness reduces organizational exposure and demonstrates program maturity to regulators.

PRE-EXAMINATION PREPAREDNESS

- [ ] Establish a standing regulatory response team with designated representatives from compliance, legal, finance, IT, and business operations.
- [ ] Maintain a continuously updated document repository containing key governance artifacts: policies, training records, investigation files, board presentations, and risk assessments.
- [ ] Conduct annual mock examination exercises simulating regulatory inquiry scenarios, including document production requests, employee interviews, and data room preparation.
- [ ] Develop pre-approved external counsel engagement protocols with rate agreements and conflict clearance procedures for rapid mobilization.

ACTIVE EXAMINATION RESPONSE PROTOCOL

- [ ] Implement an immediate litigation hold upon receipt of any regulatory inquiry, preserving all potentially responsive documents, electronic communications, and system data.
- [ ] Designate a single point of contact for all regulator communications to ensure message consistency and privilege preservation.
- [ ] Conduct daily internal briefings during active examinations to coordinate document production, track outstanding requests, and assess emerging risk areas.
- [ ] Document all interactions with regulatory authorities, including verbal communications, with contemporaneous memoranda.

Crisis Management & Rapid-Response Protocol

Compliance failures that escalate into public crises demand a structured, cross-functional response that extends well beyond the whistleblower triage framework. The CCO must lead the compliance dimension of crisis response while coordinating with legal, communications, and executive leadership.

IMMEDIATE RESPONSE (0–48 HOURS)

- [ ] Activate the cross-functional crisis response team: CCO, General Counsel, Chief Communications Officer, CISO, and relevant business unit leadership.
- [ ] Issue an organization-wide litigation and document preservation hold covering all potentially relevant records, communications, and system logs.
- [ ] Prepare initial regulatory notification drafts for applicable authorities (e.g., HHS for HIPAA breaches, SEC for material disclosure events, data protection authorities for GDPR incidents).
- [ ] Coordinate with external communications to align public statements with legal privilege considerations and regulatory disclosure obligations.

SUSTAINED RESPONSE & REMEDIATION (48 HOURS–30 DAYS)

- [ ] Commission a root cause analysis to identify systemic control failures versus isolated incidents.
- [ ] Develop and execute a targeted remediation plan addressing identified vulnerabilities, with defined milestones and executive accountability assignments.
- [ ] Prepare a comprehensive board briefing documenting the incident timeline, organizational response, regulatory interactions, and forward-looking remediation commitments.
- [ ] Conduct a post-incident review to capture lessons learned and integrate findings into the compliance risk register and training curriculum.

CCO Organizational Authority & Reporting Structure

The DOJ Evaluation of Corporate Compliance Programs explicitly assesses whether the CCO possesses sufficient authority, stature, and independence to be effective. Establishing the right organizational positioning is foundational to program credibility.

STRUCTURAL BEST PRACTICES

- ☐ **Dual Reporting Line:** The CCO should report directly to the Chief Executive Officer for operational matters and independently to the Audit Committee of the Board of Directors for governance and escalation purposes.
- ☐ **Budget Independence:** The compliance function should maintain a dedicated, board-approved budget that is not subject to unilateral reduction by business unit leadership or the CFO without Audit Committee notification.
- ☐ **Direct Board Access:** The CCO should have standing agenda time at quarterly Audit Committee meetings and the ability to request ad hoc executive sessions without management intermediation.
- ☐ **Organizational Stature:** The CCO should hold a title and compensation level commensurate with other C-suite officers, signaling institutional commitment to compliance as a strategic function.

KEY GOVERNANCE DOCUMENTS

- ☐ Board-approved Compliance Charter defining the CCO's mandate, authority, independence protections, and resource entitlements.
- ☐ Formal delegation of authority matrix specifying the CCO's decision rights for investigations, policy enforcement, and disciplinary recommendations.
- ☐ Annual compliance program effectiveness report presented directly to the Board or Audit Committee, independent of management review or editorial control.

M&A Compliance Integration

Mergers, acquisitions, and divestitures introduce significant compliance risk through inherited regulatory exposure, misaligned governance structures, and cultural integration challenges. The CCO must be embedded in the transaction lifecycle from due diligence through post-close integration.

PRE-CLOSE DUE DILIGENCE

- ☐ Conduct a comprehensive compliance risk assessment of the target entity, including regulatory history, pending investigations, litigation exposure, and prior enforcement actions.
- ☐ Evaluate the target's existing compliance program against DOJ ECCP and applicable industry-specific framework criteria.
- ☐ Assess anti-corruption risk exposure, particularly for targets operating in high-risk jurisdictions or utilizing third-party intermediary networks.
- ☐ Review data privacy obligations and cross-border transfer mechanisms to identify integration conflicts with acquirer privacy frameworks.

POST-CLOSE INTEGRATION (FIRST 120 DAYS)

- ☐ Deploy Day 1 compliance onboarding for all acquired personnel, covering the acquirer's Code of Conduct, whistleblower reporting channels, and key policy obligations.
- ☐ Harmonize governance policies within 90 days, prioritizing anti-corruption, conflicts of interest, data privacy, and third-party risk management frameworks.
- ☐ Integrate the target's vendor and third-party ecosystem into the acquirer's TPRM platform, with expedited due diligence for high-risk relationships.
- ☐ Establish a dedicated integration compliance workstream with milestone tracking and executive reporting to the Audit Committee.

Compliance Program Effectiveness Testing

KPI dashboards measure program activity; effectiveness testing determines whether the program actually prevents and detects misconduct. The DOJ distinguishes between programs that exist on paper and those that work in practice — this section addresses the latter.

TESTING METHODOLOGIES

- ☐ **Transaction Testing:** Conduct periodic sampling of high-risk transactions (expense reports, vendor payments, gifts and entertainment, charitable contributions) to verify that policy controls are functioning as designed.
- ☐ **Mock Investigations:** Simulate whistleblower reports and walk them through the full triage, investigation, and remediation lifecycle to identify procedural gaps and response time deficiencies.
- ☐ **Tabletop Exercises:** Facilitate scenario-based workshops with senior leadership simulating regulatory examinations, data breaches, and FCPA violations to stress-test organizational readiness.
- ☐ **Control Environment Surveys:** Deploy periodic pulse surveys to measure whether employees understand their compliance obligations, feel safe reporting concerns, and perceive that violations carry real consequences.

TESTING CADENCE & REPORTING

- ☐ Establish a risk-based annual testing plan that allocates greater frequency and depth to areas with higher inherent risk or prior audit findings.
- ☐ Document all testing results, including identified deficiencies and responsive corrective actions, in a format suitable for production during regulatory examinations.
- ☐ Present quarterly effectiveness testing summaries to the Audit Committee alongside the executive scorecard, providing a qualitative complement to quantitative KPI reporting.
- ☐ Engage independent third-party assessors to conduct a comprehensive program effectiveness review at least biennially, benchmarking against DOJ ECCP criteria and industry peer practices.

ESG, AI Governance & Emerging Regulatory Trends

The CCO's mandate increasingly extends beyond traditional regulatory compliance into rapidly evolving domains. Environmental, social, and governance (ESG) disclosure requirements and artificial intelligence regulation are generating new compliance obligations that require proactive program design.

ESG COMPLIANCE CONSIDERATIONS

- ☐ Monitor evolving ESG disclosure mandates, including SEC climate disclosure rules, EU Corporate Sustainability Reporting Directive (CSRD), and state-level supply chain transparency requirements.
- ☐ Coordinate with finance, sustainability, and investor relations teams to ensure ESG disclosures are supported by auditable data and internal controls comparable to financial reporting standards.
- ☐ Assess greenwashing risk exposure across marketing materials, public filings, and investor presentations to prevent enforcement actions by the SEC, FTC, or international equivalents.
- ☐ Integrate ESG-related compliance obligations into the enterprise risk register and third-party due diligence frameworks.

ARTIFICIAL INTELLIGENCE & AUTOMATED DECISION-MAKING GOVERNANCE

- ☐ Inventory all AI and algorithmic decision-making systems deployed across the organization, including applicant screening, credit decisioning, claims processing, and compliance monitoring tools.
- ☐ Establish an AI governance framework addressing bias testing, model validation, human oversight requirements, and documentation obligations aligned with the EU Artificial Intelligence Act and emerging U.S. state regulations.
- ☐ Implement transparency and explainability protocols for AI-assisted decisions that impact employees, customers, or third parties, with escalation paths for contested outcomes.
- ☐ Monitor legislative developments in AI regulation across key operating jurisdictions and maintain a regulatory change management process to integrate new requirements into existing compliance controls.

Document Retention & Litigation Hold Protocols

Defensible document retention practices are a regulatory expectation and a litigation necessity. Spoliation of evidence — whether through negligent destruction or absence of a formal retention program — exposes the organization to adverse inference sanctions, monetary penalties, and reputational damage.

RETENTION SCHEDULE DESIGN

- ☐ Develop a comprehensive retention schedule categorizing records by type (financial, employment, regulatory filings, contracts, investigation files, board minutes) with jurisdiction-specific minimum retention periods.
- ☐ Align retention periods with applicable statutory and regulatory requirements, including SOX (7 years for audit workpapers), HIPAA (6 years for covered entity records), OSHA (5 years for injury logs), and state-specific employment record mandates.
- ☐ Designate record custodians for each category with documented accountability for retention compliance and periodic certification of schedule adherence.
- ☐ Implement automated retention tagging within document management and email archiving systems to reduce reliance on manual compliance.

LITIGATION HOLD PROCEDURES

- ☐ Define triggering events for litigation holds: receipt of a complaint, government subpoena, preservation letter, regulatory inquiry, or reasonable anticipation of litigation or investigation.
- ☐ Establish a standardized hold notice process with documented acknowledgment by all custodians, including IT administrators responsible for system-level preservation.
- ☐ Maintain a centralized litigation hold register tracking active holds, scope of preservation, custodian acknowledgments, and periodic reminder cadence.
- ☐ Implement a formal hold release and destruction certification process requiring legal sign-off before resuming scheduled destruction of previously held records.

Post-90 Day Continuity & Program Sustainability

Completing the initial 90-day implementation plan establishes an operational foundation; however, program effectiveness requires continuous testing, iterative enhancement, and structural alignment with organizational expansion.

SAI360 provides an integrated enterprise solution designed to support compliance executives across every phase of program maturity:

- Policy & Learning Management: Centralize policy distribution, track employee attestations, and deploy role-based compliance training.
- Compliance Risk Assessments: Automate risk identification, scoring methodology, and corrective action plans.
- Third-Party Risk Management (TPRM): Automate due diligence, vendor risk profiling, and continuous sanction screening.
- Healthcare GRC Suite: Purpose-built frameworks addressing HIPAA, provider screening, and billing compliance oversight.

Plan Beyond 90 Days – Schedule a Demo