Skematic
An FRT Brand

PLAYBOOK

Integrating Risk Management into Your Compliance Program

ABOUT THIS GUIDE

Effective compliance programs start with risk management. Viewing compliance through this lens helps ensure your program is strategic, structured, and tailored to your firm's specific risks. By identifying risks, assigning scores, and implementing controls, teams can prioritize efforts, allocate resources, and meet regulatory expectations.

This playbook offers a step-by-step guide to managing compliance through a risk-based approach—equipping you with tools to build a resilient and defensible program.

www.skematic.com

Table of Contents

Step 1: Define the Scope of Your Compliance Program

Every CCO has experienced scope creep. Cybersecurity issues land on your desk. HR violations become compliance matters. Before you know it, your team is managing everything except what regulators actually care about during examinations. Start by creating definitive boundaries around your compliance obligations.

Key Actions

1. Catalog Your Requirements

Build a comprehensive inventory of all laws, regulations, industry standards, and contractual obligations that apply to your firm. Consider:

- **Federal regulations**: Investment Advisers Act, Securities Exchange Act, Bank Secrecy Act, ERISA (if applicable)
- **State requirements**: Registration, notice filings, books and records
- **Industry standards**: Custody rules, performance advertising, fee arrangements
- **Contractual obligations**: Prime brokerage agreements, insurance requirements, vendor contracts

Organize your inventory by regulator, jurisdiction, or client type. Each requirement should include its source and be easily accessible for updates.

Regulatory guidance evolves constantly, and what seemed like a minor requirement can become an examination priority overnight.

2. Map Internal Policies to Requirements

Every internal policy should trace back to a specific regulatory obligation. This isn't just good governance; it's essential for examination readiness. When regulators ask why a particular policy exists, you need a clear answer that goes beyond "it seemed like a good idea."

Review your existing policies and procedures. Eliminate those that don't serve a clear purpose. Strengthen those that address multiple requirements. Remember that policies create their own obligations once you put them in writing.

Sample Compliance Inventory

Risk	Source
Non-compliance with internal policies and procedures	IAA 206(4)-7
Failure to maintain adequate books and records	IAA 204(2)
Firm makes false or misleading claims in marketing materials	IAA 206(4)-1
Failure to timely update and distribute Form ADV	Rule 203A-5(b)
Risk that counterparties are in violation of the Bank Secrecy Act	Bank Secrecy Act, USA PATRIOT Act, OFAC
Employee conducts insider trading by trading in their own accounts	Rule 204a, Rule 10b-5

3. Engage Stakeholders

Compliance doesn't happen in isolation. Regular touchpoints with various functions help identify emerging risks and ensure compliance considerations are built into new initiatives rather than bolted on later.

Step 2: Build a Risk Scoring Framework

Not all compliance risks are created equal. Your resources aren't unlimited, and regulators expect you to focus on what matters most. Risk scores will make it easy to focus efforts effectively.

Key Actions

1. Define Risk Criteria

Create consistent definitions for likelihood and impact that your entire team can apply uniformly:

Likelihood Levels		Impact Levels	
Rare	Unlikely given current controls and business practices	Minor	Limited disruption, easily manageable
Possible	Could occur under certain circumstances	Moderate	Noticeable operational impact, potential regulatory attention
Likely	Expected to happen without intervention	Severe	Significant financial penalties, reputational damage, regulatory action

2. Build Your Risk Matrix

Multiply likelihood and impact to establish risk scores that drive resource allocation. Base your assessments on your firm's actual risk profile, not theoretical scenarios. A small wealth manager managing individual accounts faces different risks than a multi-billion dollar firm managing institutional assets.

Likelihood / Impact	Minor (1)	Moderate (2)	Severe (3)
Rare (1)	Low (1)	Low (2)	Medium (3)
Possible (2)	Low (2)	Medium (4)	High (6)
Likely (3)	Medium (3)	High (6)	High (9)

Here is an example of how you might evaluate, classify and mitigate different compliance risks:

Low Risk (1)

- **Example**: A small error in a non-public-facing document that is unlikely to be reviewed by regulators.
- **Impact**: No financial penalty or reputational harm.
- **Mitigation**: Standard review procedures in place.

Medium Risk (3)

- **Example:** Non-compliance with a major rule, but it applies narrowly to certain transactions rarely encountered by the firm.
- **Impact:** Potential for significant fines if discovered.
- **Mitigation:** Proactive staff training and audits.

High Risk (9)

- **Example:** Systematic failure to report trades under strict regulatory requirements (e.g., MiFID II or Dodd-Frank).
- **Impact:** Large fines, regulatory action, and reputational damage.
- **Mitigation:** Comprehensive system review and obtain outside compliance consultancy.

3. Consider Dynamic Factors

Risk scores should reflect current regulatory priorities and industry trends. The SEC's annual examination priorities provide clear signals about where additional scrutiny is likely. ESG disclosures, cybersecurity, and fee arrangements have all moved up the priority list in recent years.

Update your risk assessments when business practices change, new regulations emerge, or examination trends shift. A static risk assessment becomes less valuable over time.

Here is an example of what a prioritized risk matrix might look like (note: this is for demonstration purposes only—these scores should differ depending on each firm's risk profile):

Compliance Risk	Likelihood	Impact	Risk Score
Misleading performance claims	Likely (3)	Severe (3)	9
Books and records gaps	Possible (2)	Severe (3)	6
Failure to timely update and distribute Form ADV	Possible (2)	Moderate (2)	4
Personal trading violations	Rare (1)	Severe (3)	3

Step 3: Design and Implement Controls

Your highest-risk areas demand the most robust controls. However, controls themselves create operational requirements. Every control should be sustainable and measurable.

Key Actions

1. Categorize Controls

Structure your controls into clear categories. Sample categories might include:

Testing

Proactive evaluation of whether your controls work as designed. This includes mock examinations, sampling reviews, and periodic assessments. Testing is typically scheduled (quarterly or annually) and documented for audit trails.

Example: Quarterly review of marketing materials to ensure performance claims are compliant.

Monitoring

Ongoing oversight that flags issues in real time. Technology-driven monitoring systems can identify potential violations before they become problems.

Example: Automated alerts when employees attempt to trade restricted securities.

Training

Education that ensures everyone understands their compliance responsibilities. Training should be tailored to job functions and updated when regulations change.

Example: Annual compliance training for all employees, with specialized sessions for portfolio managers on trading restrictions.

Oversight

Governance structures that assign accountability and create checks and balances. Clear ownership prevents compliance issues from falling through the cracks.

Example: Investment committee review of new investment strategies for compliance implications.

Policies and Procedures

Written guidance that establishes expectations and processes. Policies should be practical, current, and actually followed.

Example: Detailed procedures for Form ADV updates that specify timing, approvals, etc.

2. Consider These Principles

Proportional Response

High-risk areas deserve multiple, overlapping controls. Lower-risk areas may need only basic procedures and periodic checks.

Integration

Controls work best when built into existing workflows rather than added as separate compliance steps.

Measurability

Every control should produce evidence of its operation that you can review and present to regulators.

Sustainability

Controls that require heroic efforts to maintain will eventually fail. Design for your actual resources.

Sample Control Framework					
Compliance Risk	**Testing**	**Monitoring**	**Training**	**Oversight**	**Policies & Procedures**
Non-compliance with internal policies and procedures	• Check Code of Ethics (COE) Affirmations, training completion, and violations		• Annual compliance training • Employee onboarding		• Compliance Manual • Code of Ethics
Firm makes false or misleading claims in marketing materials	• Review flagged content • Check for unapproved marketing activity and performance claims	• Email surveillance tool • Marketing pre-clearance workflow		• CCO reviews Investor Reports before distribution	• Marketing policy • Procedures for marketing review
Risk that counterparties are in violation of the Bank Secrecy Act		• Fund Administrator reviews OFAC list monthly • Due Diligence of Service Providers • Check Lexis Nexis weekly	• New Employee onboarding that includes AML Training	• Approval process for service providers	• AML Policies & Procedures
Employee conducts insider trading by trading in own accounts	• Check Code of Ethics Affirmations, training completion, and violations • Review flagged emails and expert network usage	• Personal trading tool and restricted list • Email Surveillance tool	• Annual Compliance Training • New Employee Onboarding	• Personal Trading Restricted List • Personal trade pre-clearance form • Quarterly employee affirmations of compliance with insider trading policy	• Code of Ethics • Procedures to detect and prevent insider trading • Policy on use of Expert Networks

3. Document Control Effectiveness

Regular evaluation of control effectiveness is critical for examination readiness and program improvement. This isn't a once-a-year exercise; it's an ongoing process that demonstrates the thoughtfulness of your approach. To evaluate and document control effectiveness, follow these steps:

Define Evaluation Criteria:

Set clear benchmarks for evaluating control effectiveness. These benchmarks could include:

- Is the control designed appropriately for the risk?
- Is implementation consistent and reliable?
- Does testing show the control is effective?
- Are there measurable outcomes that demonstrate impact?

Conduct Testing:

Testing is the foundation of evaluating control effectiveness. Testing methods might include:

- Walkthroughs: Review how the control operates step-by-step to confirm that it operates as intended.
- Sampling: Analyze a representative sample of transactions or activities to spot deviations.
- Simulations: Conduct mock examinations or compliance breach scenarios to evaluate control performance under stress.
- Data Analysis: Track metrics like the frequency of breaches or flagged activities.

Score Effectiveness:

Assign a qualitative or quantitative score to each control based on the findings. For example:

- Fully Effective: Well-designed, consistently implemented, achieving desired results
- Partially Effective: Generally working but with identified gaps or inconsistencies
- Ineffective: Failing to adequately address the intended risk

Identify Gaps and Weaknesses:

Document any issues uncovered during testing, such as:

- Controls that are not fully implemented.
- Overlaps or redundancies with other controls.
- Controls that fail to address the intended risk.

For each gap, note the root cause (e.g., insufficient resources, unclear processes) and the potential impact if the control is not improved.

Document Findings:

Maintain detailed records of your evaluations, including:

- Name and purpose of the control.
- The compliance risks the control is meant to mitigate.
- How you evaluated the control's effectiveness.
- The overall evaluation score of the control (e.g., a scale from 1–5 or qualitative labels).
- Supporting Evidence (data, reports, or other documentation used in the assessment).
- Recommendations or an action plan for improving partially effective or ineffective controls.

4. Calculate Residual Risk

After implementing controls, reassess your risk scores to determine remaining exposure. This residual risk calculation helps validate that your control framework is appropriate for your firm's risk tolerance.

Some risk will always remain. The goal is ensuring that residual risk levels are acceptable and that you can explain your rationale to regulators.

Sample Control Effectiveness Log					
Control	**Risk Addressed**	**Testing Method**	**Findings**	**Effectiveness Score**	**Action Plan**
Insider Trading Pre-Clearance	Insider trading by employees	Sampling of trade logs	Control generally effective; 5% of transactions lacked pre-clearance.	Partially Effective	Enhance employee training; implement reminders.
Quarterly Marketing Review	False claims in marketing materials	Walkthrough, sample audit	Control effective; no flagged issues in review.	Fully Effective	Maintain process.
Books & Records Retention	Failure to maintain adequate documentation	Simulation, data analysis	Records missing for 2 out of 20 sampled transactions.	Ineffective	Update retention policies; automate reminders.

Step 4: Implement Monitoring and Reporting Processes

Risk scoring and control design are only as good as your ability to operationalize them. To ensure your compliance program functions as intended—and can stand up to regulatory scrutiny—you need robust, ongoing monitoring and reporting capabilities.

Key Actions

1. Establish Monitoring Mechanisms

Monitoring is essential to verify that controls are working and that compliance obligations are being fulfilled on schedule. Effective programs use a combination of:

- Real-time dashboards to track compliance activities and surface overdue or high-risk items
- Exception reporting to flag anomalies for review and resolution
- Automated alerts and recurring task reminders to prevent things from falling through the cracks
- Issue escalation workflows for managing findings or incidents

Rather than relying on scattered reminders, email threads, or shared spreadsheets, leading teams implement centralized platforms to track execution. For example, purpose-built platforms like Skematic offer a centralized "compliance command center" where all activities, tasks, issues, and controls are tied

directly to underlying policies and requirements. This allows compliance teams to monitor the program in real time, rather than through retroactive audits or manual checks.

2. Develop Reporting Templates

Effective reporting brings clarity and structure to compliance oversight. Design reports that:

- Summarize the status of compliance tasks and recurring activities (what's done, what's overdue)
- Highlight high-priority risks and residual scores across business lines
- Track the effectiveness of controls and resolution of issues
- Provide clear audit trails with date-stamped documentation and approvals

Modern platforms allow these reports to be automatically generated and customized for different audiences—regulators, executive teams, boards, or internal stakeholders—so you're not scrambling to compile documentation during exams or internal reviews. With tools like Skematic, firms can instantly export reports showing execution status, policy linkage, and evidentiary documentation, eliminating manual collation and ensuring consistency across reports.

3. Foster Continuous Improvement

A risk-based compliance program should evolve with your business, regulatory expectations, and lessons learned. Build mechanisms to review and refine your framework, including:

- Post-mortems after incidents or near-misses
- Feedback loops from control testing and issue tracking
- Integration of new regulatory guidance and industry best practices
- Periodic program reviews, ideally using historical data to show performance trends over time

This is another area where technology can accelerate maturity. Systems like Skematic support version control of policies, documentation of procedural changes, and easy comparison of year-over-year performance. By tracking what changed, why, and whether it improved your compliance posture, your team can present a defensible, proactive approach to regulators—and demonstrate strategic leadership to the business.

System Capabilities

While each firm's monitoring stack may differ, certain capabilities are foundational, and should be sought after in a compliance management tool.

System Feature / Capability	Purpose
Compliance dashboards	Visualize task completion, risk heatmaps, and control effectiveness
Incident/case management	Track findings, action plans, and resolution status
Audit trail logging	Preserve documentation of who did what, when, and why
Collaborative workflows	Reduce email noise and centralize reviews, approvals, and comments
Policy-to-activity linkage	Show direct evidence that procedures are executed as required

Platforms like Skematic combine all these elements into one integrated compliance operating system. Built specifically for financial services compliance teams, Skematic enables real-time program oversight and produces "regulatory receipts" that simplify responses to exams or audits. By embedding controls, evidence, and reviews into a connected framework, firms move beyond reactive reporting to strategic, real-time program management.

Conclusion

Risk-based compliance is more than a framework—it's a mindset. By identifying specific obligations, assigning risk scores, applying tailored controls, and continuously monitoring performance, firms can manage compliance in a way that is defensible, scalable, and aligned with regulatory expectations. But success doesn't come from risk scoring alone. The true challenge lies in how these frameworks are implemented and maintained across teams, time periods, and evolving requirements. Without structure, even well-designed programs can become inconsistent or difficult to evidence.

Use this playbook as your guide for applying a risk-based approach to your compliance efforts—and consider how your systems, workflows, and documentation practices can support long-term program integrity and adaptability.

About Skematic

We believe compliance teams deserve better. While regulated industries face unprecedented scrutiny, compliance professionals have been held back by outdated tools. Skematic changes that by integrating the people, processes, and systems that power modern compliance programs.

Our platform is the engine behind your existing compliance framework. We empower compliance professionals with a unified environment for collaboration, accountability, and reporting. With Skematic, you can finally sunset the fragmented mix of spreadsheets, emails, and disconnected tools, replacing them with a purpose-built solution that makes compliance teams look good – to regulators, investors and internal stakeholders alike.

skematic.com | info@skematic.com | +1 (781) 887-0539