Diligent

Best Practices for Building a Culture of Compliance:

4 Focus Areas for Strengthening Policy Management & Compliance Training

Introduction

With an evolving regulatory landscape, increased attention to political and social issues, and heightened attention to incidents and whistleblower protections, the past five years have demonstrated that merely checking the box on compliance is no longer enough. Corporations who do not take a proactive approach risk serious financial and reputational damage.

The United States Department of Justice (DOJ) has intensified its scrutiny as well. In April 2019, the DOJ published its Evaluation of Corporate Compliance Programs guidance — a significant expansion of the earlier guidance published in 2017. With more discussion regarding what effective compliance programs should achieve and what prosecutors want to see from companies under regulatory scrutiny, it is a valuable resource for compliance officers and directors who want to ensure their compliance programs satisfy regulator expectations.

On June 1, 2020, the DOJ updated this guidance document once again to reflect, as then-Assistant Attorney General Brian Benczkowski said, "additions based on our own experience and important feedback from the business and compliance communities."

The changes, while not extensive or surprising, do indicate increased understanding by the DOJ of the variation in circumstances in which corporate misconduct occurs and the areas in which prosecutors should focus their inquiries. Specifically:

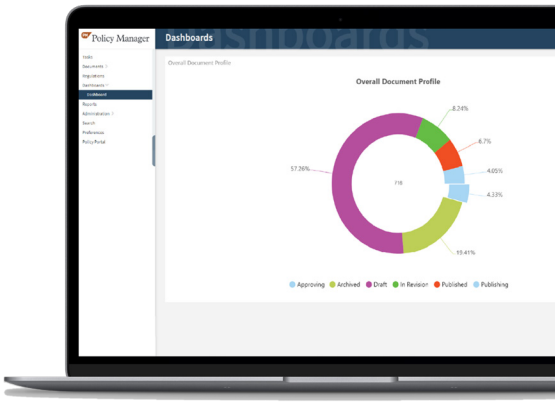
- **Is the corporation's compliance program well designed?**
- **Is the program being applied earnestly and in good faith — adequately resourced and empowered to function effectively?**
- **Does the corporation's compliance program work in practice?**

Internal compliance teams face many challenges in addressing these questions and adapting to a changing landscape in a timely fashion: disparate policies and processes scattered across the organization, manual processes that slow things down and employee resistance, to name a few.

Where should teams focus first?

Read on for best practices in four priority areas when building and fine-tuning an internal compliance program.

1. Policy Management



Strong, well-managed policies are the lifeblood of compliance and growth. They define, articulate and communicate expectations, communicate risk limits, explain governance and accountability, and guide desired conduct. They're essential to creating a culture of compliance, protecting the business and achieving business objectives.

Yet in today's world of rapidly changing mandates and evolving business strategies, organizations are challenged to manage hundreds or even thousands of policies. Often, these policies are scattered across the enterprise with no central repository, inconsistent styles, lack of ownership and poor lifestyle management — from insufficient mapping, to exceptions and incidents, to a lack of cross-referencing standards, rules and obligations.

If a company can't keep a firm grip on how its policies and procedures are implemented, room emerges for measures that don't reflect a commitment to strong ethics and compliance. Maybe a procedure neglects to collect a piece of data crucial for regulatory compliance. Or perhaps more nefarious practices emerge, such as putting whistleblowers on probation and nudging them out the door.

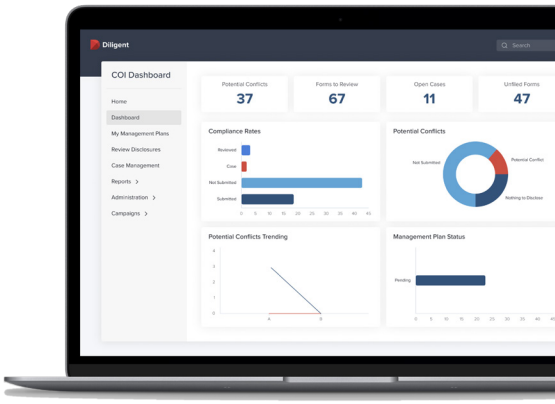
The DOJ will be taking notice. Are your policies and procedures published in a searchable format for easy reference? Does your company track access to see which policies are getting the most employee attention?

Policy Management: A Best Practices Checklist

Your organization's policy management is strong if it includes:

- ☐ An overall policy management process in which policies and procedures relating to the compliance program are made readily available to employees
- ☐ A "policy about policies" to ensure all are structured in a uniform way that doesn't confuse employees or third parties
- ☐ A system of review and attestation for new or updated policies
- ☐ A thoughtful approach to exception requests, since a zero-tolerance standard can drive some parties to keep quiet about mistakes rather than speak up
- ☐ Procedures that reflect how the business works, so employees see them as something to follow rather than something to evade
- ☐ An integrated, streamlined policy management platform, enabling you to regularly update policies with changing regulations, track and manage employee engagement and training, and reduce your organization's exposure to noncompliance risks
- ☐ Model and evaluate pay-for-performance plans and measure compensation according to relevant performance metrics

2. Conflicts of Interest (COI) Management



Conflicts of interest are at the root of many business ethics and regulatory compliance problems. Even if a conflict isn't impermissible from a regulatory or fiduciary perspective, this conflict — whether actual or perceived — can hurt your organization's reputation. Politicians, prosecutors and the press frequently seize on COIs as suggestive of institutional malfeasance. Meanwhile, regulatory bodies such as the Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), the Internal Revenue Service (IRS) and the National Institutes of Health (NIH), as well as myriad anti-corruption statutes worldwide, are increasingly requiring COI management programs.

Organizations navigating this landscape face many challenges: lost forms, employee delays and reluctance, and more. One big challenge is process. COI management is quite difficult when done with manual processes. If you simply have people fill out forms and then you store those forms in a filing cabinet, you'll never be able to follow up on those issues effectively. And if you have dozens of people listing hundreds of COIs, it becomes very difficult, if not impossible, to monitor conflicts.

The risks are high for COI mismanagement. If your company collects COI data but never follows up, that could be used against the company should the enforcement community ever investigate a potential problem. Furthermore, as companies continue to broaden their COI rules and push disclosure requirements deeper into the enterprise, the number of participants and the risk of mishandling a COI increase.

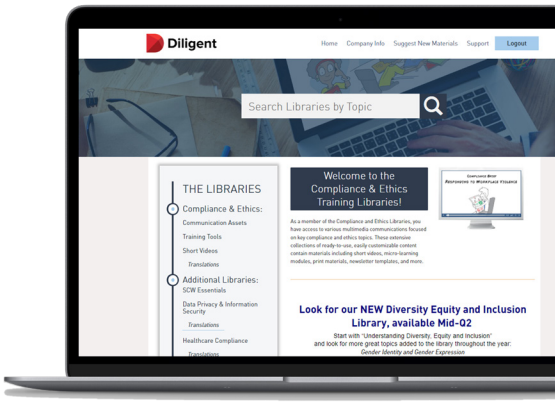
In terms of organizational culture, the COI process can be delicate. People who must share potential COIs can become defensive. If the company isn't efficient in addressing COIs, you could exacerbate employees' sensitivity to the COI process.

Conflicts of Interest Management: A Best Practices Checklist

Your organization's COI management is strong if it includes:

- ☐ Clear, board-approved COI policies
- ☐ Disclosure surveys that are comprehensive, appropriate to different audiences and easy to understand
- ☐ A process for regular information collection and a formal structure for objective review
- ☐ Training materials and executive communications
- ☐ "Smart forms" that make COI disclosures easier to submit. Look for automatically adjusting questions and pre-filled answer fields based on past responses
- ☐ A central COI repository
- ☐ An automated review process, with automated flagging and reminders to keep things moving and tracking to make sure actions happen in a timely fashion
- ☐ An audit trail, which electronic COI solutions should generate automatically
- ☐ An independent audit at a fixed interval, say every three years
- ☐ A dashboard summary of compliance metrics, ideally with interactive visualizations and customizable, real-time reports
- ☐ Data analytics for understanding employee behavior and improving policies, procedures and internal controls
- ☐ Stringent data security and data privacy with multiple layers of physical and logical protection: encryption, GDPR-ready processes, an ISO-certified hosting facility and more

3. Incident Management and Whistleblower Support



Incident management is a company's ability to receive or intake an allegation about an event or action. The goal for an organization is to convey that it has heard the complaint and taken the appropriate steps to investigate and rectify any problems the company finds.

It's an increasingly high-stakes goal. Under legislation such as the Sarbanes-Oxley Act or the
Dodd-Frank Act, just about every large company is required by law to have a system for internal reporting of misconduct or similar concerns. Companies are required to document their processes for incident reporting, and outside auditors can demand spot checks where they select numerous cases at random and review how those incidents were handled.

These audits and external reviews can be extensive. Auditors will want to see all the work the company has done, the supporting evidence, investigative materials, what steps were taken to remediate and so forth. And companies that don't produce those things are at risk of enforcement, with legal and financial impact, from the DOJ.

Furthermore, failure to protect whistleblowers exposes companies to litigation and enforcement risk under the Dodd-Frank Act, the False Claims Act and other statutes. Aggrieved employees can also bring civil lawsuits themselves; so even if the business ultimately prevails, corporate time, money and focus are still spent on litigation rather than on more productive tasks.

Establishing a whistleblower hotline is no longer enough. Nor are the disparate manual processes for incident management at many corporations. With tracking allegations and follow-up by spreadsheets,
for example, there's great potential for error — and, more importantly, there's no way to enforce a series of repeatable steps.

Another big pitfall: lost investigations. When the institution doesn't know the status of the investigation, it can't take any mitigating steps.

Organizations need to coordinate the efforts of investigators looking into the allegation, managers who might be talking with the people who originally reported the issue and other employees taking remediation steps to fix the problem. All of this is extremely difficult to do manually, especially at large volumes.

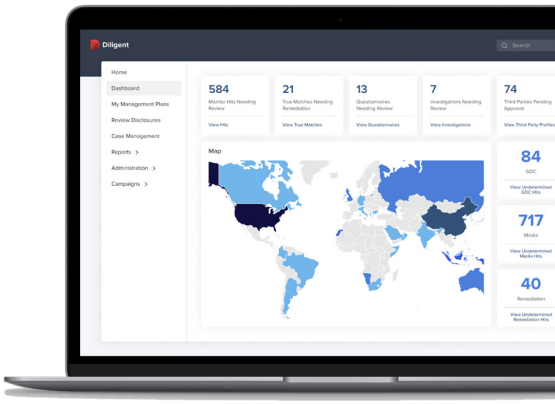
Incident Management and Whistleblower Support: A Best Practices Checklist

Your organization's incident management and whistleblower programs are strong if you're taking a multipronged approach spanning training, reporting and incident management, with full transparency into your corporate policies and code of conduct.

This includes:

- ☐ Broad intake capability, so people can submit allegations by email, telephone hotline, website, text messaging, a kiosk on the factory floor or even just by talking to their manager
- ☐ Consistent protocols for incident management, with all materials from the investigation attached electronically to a single master case in an easy-to-search fashion, so you're not losing any important details
- ☐ Scalability features like automatic task assignment, so you can effectively handle hundreds — or even thousands — of incidents at one time
- ☐ Flexibility in areas like intake form design and customizable workflows to accommodate for twists and turns in operations
- ☐ Case management automation to keep teams moving and free investigators to focus on the case. An automated system can also give you a full audit trail for every incident, so you'll always know what steps were or weren't taken.
- ☐ Incident reporting that's secure, mobile-accessible, easy to operate and allows anonymous reporting for whistleblowers and sharable dashboards and reports for case managers

Compliance and Ethics Training



A company's compliance training covers topics that have serious ramifications for individual employees as well as the business. Yet many employees see such training as fundamentally uninteresting, irrelevant or just plain boring.

Why is this the case?

The problem starts with traditional, long-format, once-a-year training with legalistic content in antiquated formats. This has proven ineffective and elicited poor responses from employees. Compliance training materials often suffer from obscured or nonexistent takeaways. After spending 30 minutes on an e-learning training session, employees won't necessarily know what they should do in a challenging situation. Today's tech-savvy workforce sets the "effectiveness bar" even higher; gaining their attention and keeping them engaged requires video and graphics with high production values. They also expect to access your training content wherever and whenever they want it.

A significant level of "training fatigue" has settled like a pall over compliance programs. Employees may feel they are over-trained in courses that are too long and that cause interruptions in productive workflow, which can foment attitudes of resentment and resistance.

At the same time, employees may actually be under-trained due to courses that:

- ⊗ Occur too infrequently for content retention
- ⊗ Dwell in the realm of the theoretical and lack practical application to their daily activities
- ⊗ Do not include any meaningful follow up and reinforcement

To complicate matters even more, often when a specific area of risk is identified, a Band-Aid training solution may be hastily applied that is neither strategically targeted nor thoughtfully integrated within an overall compliance communication solution.

In short, organizations face many tough challenges in delivering compliance training, yet failing to engage employees could increase the risks of unethical or noncompliant behaviors.

What Effective Compliance Training Looks Like

Effective compliance training provides guidance not only on what not to do, but also on what to do. It gets right to the substance of the matter, presenting a common situation and the steps a person should take if/when they encounter it.

One example is training that blends education about company priorities and regulatory concerns ("don't bribe government officials," "assess the security of third-party tech service providers") with the policies and procedures the company uses to pursue operational goals.

Merely training employees on what a regulatory risk is and telling them the risk should be avoided fails to instruct them on how to avoid it. "Risk-based training" also appreciates that the challenge can sometimes be a serious regulatory issue (data security, for example) or a powerful group of people (senior executives able to override controls). Then training is tailored to the gravity of the risk: more extensive coursework, in-person sessions rather than online videos, and so forth.

But this is only one part of the solution. To tackle employee resistance and increase employee engagement, organizations need to incorporate behavior change and "microlearning" into their compliance training.

Microlearning is used for targeted instructional design that engages your learners, improves their retention and, most importantly, drives them to change their behavior patterns. Even when long-form training is necessary for deeper topics, such as bribery or fair competition rules, microlearning reminder tools can support the message.

In short, using behavior science and microlearning in compliance training means presenting engaging content that employees actually look forward to seeing, using strategic and frequent communications to reinforce this content, and incorporating tools for all learning styles, from short videos to microlearning modules, case studies and cartoon strips.

Best Practices for Incorporating Behavior Science and Microlearning Into Your Training Program

- ☐ Deliver training through experiences that last no more than from 30 seconds to three or four minutes, which can easily be incorporated into the workday
- ☐ Present interesting multimedia content with scenarios that make abstract compliance issues more concrete and relatable
- ☐ Anticipate a variety of learning styles: visual, auditory, reader/writer and kinesthetic
- ☐ Optimize training to match attention spans, lapses and spikes
- ☐ Prevent cognitive overload through presenting one learning objective per lesson
- ☐ Combat knowledge decay, which begins immediately after training, with frequent reinforcement via videos, infographics, memes, intranet blog posts and newsletter articles
- ☐ Track participation

In Conclusion

As the regulatory landscape evolves and scrutiny intensifies, technology solutions can help compliance departments keep up, even amid constrained resources and funding, by streamlining and strengthening policy and COI management, expanding incident response and whistleblower support, and using behavior science to deliver more engaging training.

Take the next step forward for your internal compliance program.
Schedule a meeting with Diligent today.

About Diligent Corporation

Diligent is the leading governance, risk and compliance (GRC) SaaS company, serving 1 million users from over 25,000 customers around the world. Our innovative technology gives leaders a connected view of governance, risk, compliance and ESG across their organizations, sparking the insights they need to make better decisions and lead with purpose. Learn more at diligent.com

For more information or to request a demo:
Email: info@dligent.com • Visit: diligent.com