Operationalize Compliance

Focus on trends and patterns to influence behavior

A WHITE PAPER FROM OVERSIGHT

Chief Compliance Officers (CCO) and compliance practitioners listen when regulatory authorities communicate their expectations around compliance. So, when the DOJ emphasizes the requirement to operationalize your compliance program, you take note. The challenge is figuring out how to integrate compliance with operations.

It is in having a functioning corporate compliance program that the DOJ will give credit.

Most companies have the basics covered – training programs, hot lines, vendor credentialing among others. They care about bribery and corruption, but too often their compliance program is not an integral part of business operations. They have existing controls in place, but data silos and manual processes create a risk where non-compliant spending and behavior could fall through the cracks.

To operationalize compliance, the approach needs to be easier and better for both the compliance team and for operations. It needs to focus on the people, their spending trends and patterns. A truly operationalized compliance program will translate into action and influence behavior for the benefit of the business.

Operationalizing compliance starts with using your data to improve internal processes and boost decision-making quality. This is done by identifying issues that improve business efficiency while enhancing the organization's ability to combat bribery and fraud.

4 Steps to Operationalize Compliance

There are four steps CCOs need to take with the business to operationalize compliance.

Step 1: Curate the Data.

Companies' data stores exist in silos today. Accounts payable data is in the ERP system; expense reporting data is in the expense management system; corporate card data is with the credit card vendor; employee records and payroll are in a HRIS, and so on. No one has a holistic and shared view. Companies need to cut across these silos of data in order for compliance to have an accurate view of what is going on in the organization. This requires collecting data sets from disparate internal and external sources, and curating them into a coherent data set.

Step 2: Analyze the Data Accurately.

The ever-growing stores of information to monitor makes it difficult (if not impossible) to identify patterns of behavior via traditional analytical approaches. The manual processes that companies employ are time-consuming and the quality of analysis is variable. They often just review a "slice in time" sample or a subset of transactions, and rely too heavily on manager review of activities as a control, which can be an ineffective rubber stamp. These traditional approaches can miss the patterns of inappropriate behavior that often occur just below their review threshold. They are not enough to effectively detect

Advanced AI-based Data Analytics vs. Traditional Auditing

Analyze all expense reports, card transactions, invoices, vouchers, and payments		Random Sampling
Compare transactions over an extended time period	VS.	Looking at one at a time in isolation
Run multiple analytics in parallel		Running one test at a time

and prevent bribery schemes that violate anti-bribery/corruption regulations. As a result, bad actors fly under the radar and too often get away with policy violations.

To find concealed violations, the system needs to automatically compare transactions over an extended time and run multiple analytics in parallel. For example, when a vendor invoice comes in, it should be analyzed for inconsistencies with previous bills, round dollar amounts, and origination from a high-risk account – potential indicators of suspicious activities. Artificial Intelligence (AI) techniques can bring all these clues together to identify risks in real-time and to find the root cause of behavior that needs to be corrected.

Step 3: Remediate Issues.

Most risk comes from very few employees and vendors. Only 10 percent of employees cause 99.9 percent of all high-risk activity in Travel & Expense. The power of advanced analytics is operational teams can spend time correcting issues among the small number of actors that are causing the problems, instead of spending the bulk of their time trying to find the issues. If the system detects a high-risk activity, it automatically assigns it to the compliance/internal audit team for remediation. A workflow system can facilitate the remediation process for operations and compliance by logically prioritizing and presenting issues, providing a relevant data for research, and documenting resolution steps. It also enables better communication with employees and internal stakeholders.

Step 4: Document, document, document.

From a compliance standpoint, if it's not documented, then it didn't happen. An operationalized compliance program can easily demonstrate to the C-suite, the board, and if necessary, to the regulators that there is consistent and proactive monitoring of all transactions for compliance risk, as well as any actions taken on the exceptions. The automated monitoring activities should be recorded in a permanent audit log. As the Morgan Stanley case demonstrates, the government will be more favorable in its rulings with companies that have been able to demonstrate such capabilities.

Reducing risk with automation

The Morgan Stanley case has proven that regulators will reward a well-defined, robust, dynamic and operational compliance program. The degree to which organizations can achieve a consistent culture of compliance, persistent training, and continuous adaptation is generally contingent on attacking the heavy lifting with automation.

An effective automated transaction monitoring program requires efficient identification of potential violations and swift remediation. Implementing AI-based technology that provides compliance professionals and operations with a centralized system that automatically inspects all transactions in a consistent manner can mean the difference between exoneration and facing criminal and civil charges.

Transaction monitoring is a critical element of an operationalized compliance program, but that can be easier said than done in our current digital age.

Case study: Morgan Stanley

When the DOJ investigated Morgan Stanley's former managing director Garth Peterson, who pleaded guilty to evading the company's internal controls, it was Morgan Stanley's operationalized compliance program that ultimately led to the DOJ's decision not to bring any enforcement action against the company.

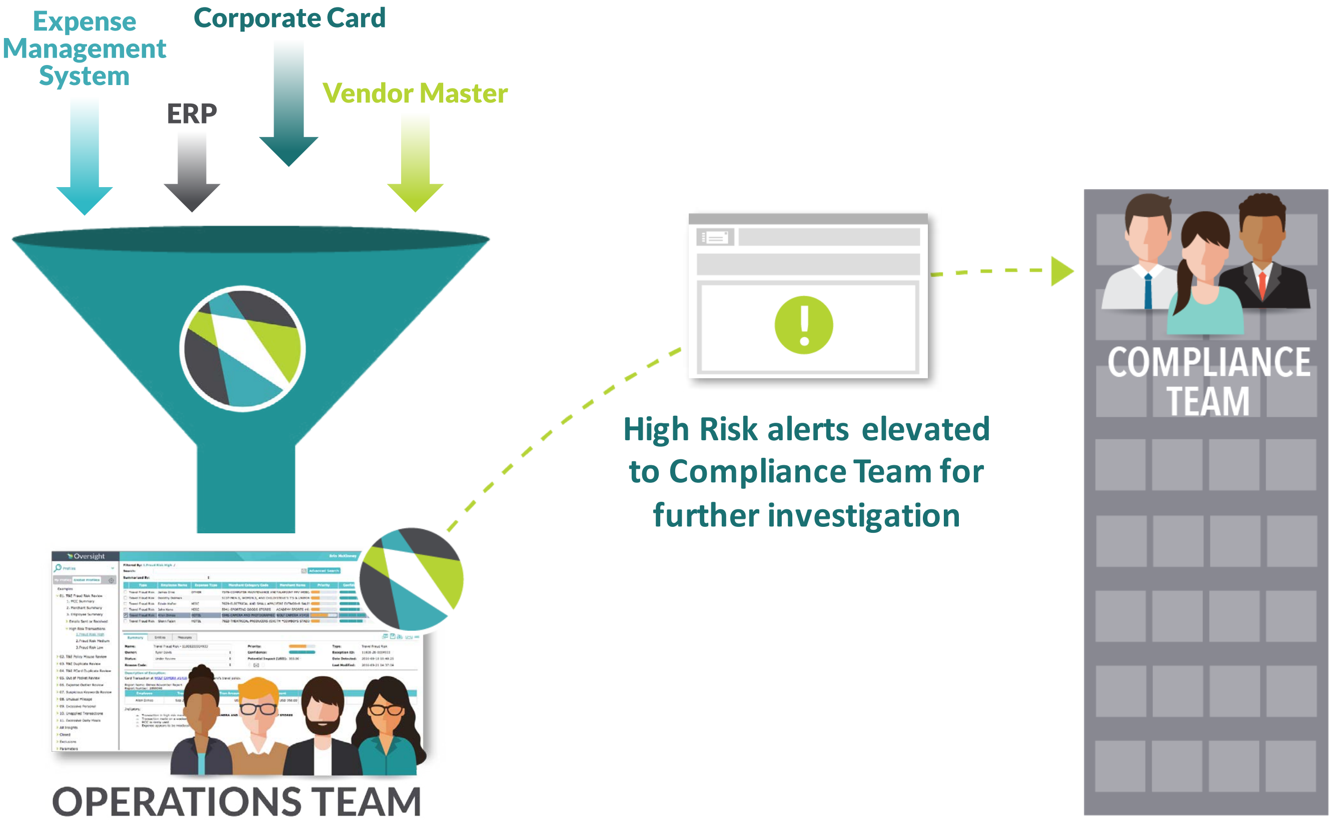
In fact, the Morgan Stanley case can serve as the model any organization can follow because it demonstrates the need to implement and follow best practices such as:

- ***Document everything:*** **Morgan Stanley maintained a system of internal controls meant to ensure accountability for its assets and to prevent employees from offering, promising or paying anything of value to foreign government officials.**
- ***Conduct regular program auditing:*** **Reviewing and updating its internal policies enabled Morgan Stanley to ensure all policies and procedures were being followed, eliminating the risk of non-compliance and eliminating FCPA risk.**
- ***Educate employees:*** **According to court documents, Morgan Stanley between 2002 and 2008 trained various groups of Asia-based personnel on anti-corruption policies more than 50 times. In fact, Peterson received training seven times and was reminded to comply with the FCPA at least 35 times.**
- ***Implement global financial systems controls:*** **Morgan Stanley provided documentation that compliance personnel regularly monitored transactions, randomly audited particular employees, transactions and business units, and tested to identify illicit payments.**

Oversight's approach to operationalize compliance and mitigate risk

A key factor that differentiates Oversight AI from traditional auditing approaches is that we provide a centralized system that inspects all transactions in a consistent manner versus the traditional sampling approach.

From the analysis, we precisely identify anti-bribery/corruption risk in the form of exceptions that require investigation and resolution. Compliance and operational teams access our system via a web browser, and they take action on the exceptions using an integrated workflow with built-in email and audit trail functionality. The system automatically tracks the steps taken to review, research, and communicate with employees and other internal stakeholders.


Expense Management System
Corporate Card
ERP
Vendor Master
High Risk alerts elevated to Compliance Team for further investigation
COMPLIANCE TEAM
OPERATIONS TEAM

As a result, our clients have been able **to significantly reduce compliance costs in this area, on average over 50 percent**. They've also increased their coverage to a 100 percent analysis of transactions and subsequent review of risky activities. And best of all, they've made a major enhancement to their anti-bribery/corruption risk detection capabilities.

What's more, one of the most beneficial aspects of implementing continuous analysis to monitor transactions along with a remediation process is the deterrent effect. Research shows that people behave differently when they know they are being watched. This "Hawthorne Effect" has resulted in a **reduction in out-of-policy transactions of up to 70 percent** in Oversight customers who routinely monitor and analyze transactions. Not only does the knowledge of an investigation serve to make employees less likely to violate company policy and regulatory laws, it also sets a tone at the top: violations will not be tolerated.

Finding well-hidden compliance violations requires the ability to analyze all expense reports, card transactions, invoices, vouchers and payments, not a sampling. Comparing transactions over an extended time horizon is better than looking at one at a time in isolation. Running multiple analytics in parallel versus running one test at a time is more efficient and effective. This enables forensic detection of patterns of behavior similar to what is done during later stages of an actual investigation.

An off-the-shelf transaction monitoring software solution may be the most cost effective alternative if it can be configured to cover your specific risks. Key evaluation criteria for an off-the-shelf transaction monitoring system include:

- □ *Can the system import data from the multiple sources in your environment?*
- □ *Are there a sufficiently wide range of analytic capabilities to identify the various indicators of risky activity?*
- □ *Will the system synthesize clues to identify employees and vendors exhibiting patterns of high-risk behavior?*
- □ *Does the case management capability handle workflow, communications, status reporting, and an independently verifiable audit trail?*
- □ *How much effort is required to customize analytic parameters (i.e. keywords, MCC risk, etc.)?*
- □ *Is the solution sufficiently turn-key to minimize the allocation and management of resources?*

While there's no guarantee that you'll be able to prevent bad actors from circumventing controls, with Oversight AI you can identify potential anti-bribery/corruption violations and operationalize compliance.

Ready to see Oversight AI in action?

SCHEDULE DEMO

Why You Need Oversight AI

You already know how important it is to have a defensible FCPA compliance program. But what if you could find an easier way to identify risks that fly under the radar?

Oversight AI is a web-based Artificial Intelligence solution that automates spending program compliance by comprehensively analyzing expense report, purchase card, and accounts payable transactions to identify fraud, non-compliant purchases, and inefficient and wasteful spending. Oversight allows you to proactively monitor business transactions for FCPA risk, identify employees exhibiting patterns of potentially improper behavior or collusion, and act on exceptions. Our solution enables you to demonstrate an effective FCPA compliance program to your executives, board and, if necessary, to the government.

Oversight makes a difference within the companies it serves, and has the experience to prove it, analyzing $2 trillion in expenditures annually at Fortune Global 5000 companies and government agencies. Oversight's solution is strengthened by partnerships with Acquis, Concur, Mastercard, Oracle, SAP and TSYS.