Keys to Successfully Adopting an Integrated Risk Strategy

INTEGRATE THE LINES, MITIGATE THE RISK.

Oversight
Nothing gets by you now™

Integrated Risk Strategy Defined

As more organizations select AI-powered platforms to help manage enterprise spend risk, adoption of an integrated risk strategy is emerging as a best practice for connecting the three lines of defense and forming more effective risk management teams.

The Three Lines of Defense in Risk Mitigation:

Finance operations teams
own and manage risk.

Compliance teams
oversee risk management.

Internal audit teams
provide independent assurance.

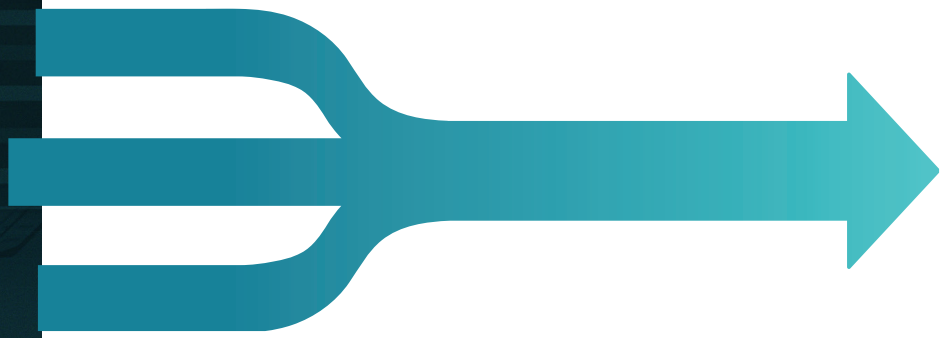
Integrate the Lines, Mitigate the Risk.

The three groups tasked with managing risk mitigation in enterprise organizations operate with little connection or interaction.

An organization's operations teams ensure that submissions are in line with company policies and self-check for fraud and waste, serving as the first line of defense in the enterprise. Conjointly, compliance teams monitor the implementation of risk management practices via operational management, searching for any evidence of fraud and waste, and ensuring regulatory controls like anti-bribery and anti-corruption, are in place and effective. On top of these efforts sits the third line of defense, the auditors who verify compliance efforts.

The groups conduct varying degrees of audit. Operations teams often conduct manual sample audits on a monthly basis, while compliance and internal audit teams perform semi-annual or ad hoc audits. None of the teams consult or meet with regularity. The entire review process exists as periodic checks by siloed groups, and as a result, it fails to catch risk and prevent recurrence effectively.

To introduce more efficiency into spend audit reviews, most organizations focus on making existing processes a little faster. An integrated risk strategy re-engineers processes to fit the desired outcome of systemic risk elimination. The result is a unified approach that works across departments, aligning the three lines of defense into a single, three-tiered risk management effort that enables communication and the sharing of intelligence for a more offensive stance.



A Shift Left in Controls

The key to success for unified risk management teams? The platform.

A spend management platform enhances communication between the three lines of defense by creating a single view of risk. It provides a shift left in controls that gives operations teams strong forensic analysis capabilities to support compliance and internal audit.

Achieving this shift, requires the ability to monitor 100% of spend. AI and advanced analytics can power the monitoring and analysis of transactions and provide finance teams with full visibility into spend data, far surpassing what is possible with manual, ad hoc reviews.

With enhanced front-end analysis, operations teams can identify spend risk early and then escalate issues that require the attention of compliance and internal audit teams. From simple duplicate payments and miscoded expense items to possible patterns of misconduct, internal fraud or signs of regulatory risk, an integrated strategy gives organizations a continuous running control to better detect and address suspicious activity.

The Benefits of an Integrated Risk Strategy:

- Eliminates manual, high-effort and low-value work
- Continuous monitoring and controls replace retroactive fact-finding expeditions
- Faster identification and resolution of risk to prevent financial loss and reputational damage by focusing on outcomes and patterns
- All three lines of defense operate more strategically to support spend management and risk mitigation

The Current State of Spend Risk

In organizations today, the assessment of spend risk is initiated when employees submit expense reports into expense management systems. A processor reviews these inputs. It's an exercise in the examination of individual expense reports, one at a time.

This type of analysis largely confines the reviewer to uncover clerical or administrative findings like missing receipts, incorrect codes or one-off cases of personal expenses. Teams are not optimized to detect anything beyond these low-level errors.

Finance operations teams tends to focus on administrative tasks:

- Is this report accurate?
- Are receipts attached?
- Are expenses coded correctly, i.e., lodging, meal expenses, etc.?

The average processor only sends back 5-15% of reports to employees for revision. Of that small percentage, 80% are sent back to correct low-risk issues (missing receipts and other minor errors). Approximately 20% of the time, processors send reports back because they believe that the expense is non-reimbursable. Yet, 90% of reports processors return because of possible non-reimbursable expenses are later approved by managers anyway.

80%
of reports are sent back for simple updates or revisions

20%
are are rejected because the expense is non-reimbursable

9 out of 10
of these end up being approved by a higher level manager

Compliance audits search for violations months later

Compliance teams conduct ad hoc fact-finding missions, reviewing a small sample of all reports in search of fraud, waste and misuse. These reviews often occur 6-12 months after the transactions. For the second line of defense, time is primarily spent looking for infractions, not remediating issues.

Internal audit provides assurance

Most bad actors in an organization are discovered through channels other than expense processing or compliance audits. It's often only after flags are raised elsewhere in the organization that internal audit teams investigate and find fraud, waste and misuse.

Upending the Current State

An integrated risk strategy process identifies high-value, ongoing, patterned or strategic risk. Teams are optimized to find duplicate payments, interdepartmental discrepancies, fraud, waste and misuse with ease.

By shifting the three lines of defense into proactive roles, risk management in the organization becomes an AI-powered, real-time effort. The proactive approach means fewer departmental siloes, a greater cultural shift towards compliance, and a reduced lag in the identification of issues that can lead to financial loss and compliance concerns.

Spend risk platform monitors 100% of transactions in the business and across departments, utilizing AI-powered tools to identify abnormal payments, errors in reporting, coding, fraud, misuse and waste, all automatically.

100% of abnormal findings are flagged, scored and evaluated by processors. Those flagged findings that fall above a certain risk threshold are directed to compliance and internal audit teams, and all risk is managed and mitigated in real-time, not months later.

Compliance audit teams sample and ensure the process is working effectively.

Internal audit teams oversee with a holistic view.

Teams meet and communicate about key findings in the platform regularly, and all three lines of defense work together to monitor and triage risk in tandem.

CLIENT SPOTLIGHT

S&P 100 Pharmaceutical Company

Business Challenge

Prior to mobilizing Oversight, and adopting an integrated risk strategy, one global biopharmaceutical company deployed a risk strategy characterized by quarterly monitoring of 1% of transactions, selected at random.

Solution

When the organization went live with Oversight in the fall of 2019, the team immediately discovered new exceptions through improved data analytics. As such, the pharmaceutical giant redesigned its spend management processes to include more coordination and communication between the lines of defense.

At the core of their redesigned processes was the continuous monitoring of expenditures. With Oversight, the organization found it possible to enhance governance and control, increase risk mitigation, and identify efficiency opportunities.

To achieve their goals, the departments took a team focus on how they assigned exceptions identified by Oversight, dividing assignment by type across the three lines of defense. The organization also installed communication parameters between the teams, so that the departments not only worked together but interacted throughout the process.

Results

The results were clear and immediately successful. The pharmaceutical industry titan redefined its Business Control Function team as a 100% risk-based department. The coordinated effort across various business groups eliminated risk and identified waste. Thanks to the Oversight platform and interdepartmental coordination, the organization sits at 100% analysis of data and reports 70% efficiency over the former process.

The pharmaceutical industry titan redefined its Business Control Function team as a 100% risk-based department.

How to Adopt an Integrated Risk Strategy

There's a misbelief in the marketplace that the highly administrative and clerical audit processes in place today is valuable in mitigating risk, waste and fraud when, in fact, they are not. With an integrated risk strategy, each line of defense becomes far more valuable.

Operations shifts focus towards optimizing spend and employee experience.

Compliance ensures continuous control and remedies issues.

Internal Audit reviews processes and technology to ensure controls work effectively and adapt over time.

Questions for consideration

- Are you making informed policy decisions based on spend data?
- Is your organization spending more time looking for misconduct than remediating it?
- Are you discovering misconduct within your spend programs through other channels, i.e., caller hotlines?
- Are you interested in elevating the role of your financial and operations teams?
- Is your operations team able to drive changes in employee policy compliance?

Find Your Place on the Curve

Every organization has its unique place on a maturity curve, and each has distinctive resource and budgetary constraints to consider. Regardless of your place on the curve, the value of integrated risk strategy is attainable for your organization with a few key steps:

1. **Begin regular meetings with the three lines of defense.**
Regular communication creates understanding among these three functions to ensure efforts align.

2. **Scrutinize the process.**
Consider what each group is doing today, and the actual outcomes each group delivers. By understanding existing processes, shortcomings and potential areas for growth, you can define a go-forward strategy.

3. **Set realistic goals.**
60, 90, and 120 days out. Move the needle from administrative oversight to spend optimization, and from highly involved data mining to strategic issue resolution one step at a time.

4. **Adopt formalized self-governance practices.**
In leading organizations, these three groups operate independently. At some periodic cadence, each line of defense peer reviews the other, monitoring the effectiveness of processes and frameworks.

5. **Lastly, ensure your technology is in place.**
The technology at the heart of your risk strategy is foundational. If your organization has not put technology in place yet to assist you in this journey, you will quickly reach a limiting plateau on how far you can go with manual effort.

The ROI of Integrated Risk Strategy

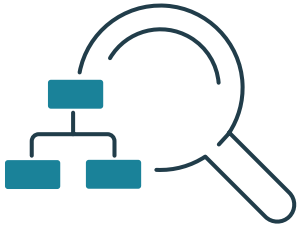
With the right solutions in place, risk is easier to detect. It's the culture change that takes steady application. Those that stay the course boast notable results.

With an integrated risk strategy, organizations can more confidently operate with the following drivers of a return on investment:

- An assurance of preventative financial controls in place, and the avoidance of future fraud and waste.
- Operational savings bolstered by identification of fraud, misuse and waste, along with errors like duplicate payments.
- The teams and tools in place to drive optimal spending.

Optimize Spend

Influence Behavior



Address Root Causes

Early Results

Within three months of deployment, operations teams can move from simple administration duties toward the more positive effort of influencing corporate culture. In those first three months, operations teams are made aware of black and white risk findings, like duplicate payments, or other occurrences outside the expected norms. With quick financial victories in hand, it's easy to begin showcasing the ROI of an integrated risk strategy to stakeholders.

Long-term Results

Over time, teams can also transition from black and white issues to gray, identifying scenarios that require more nuanced operational judgment. As operations teams can quickly dispatch duplicates and errors, they can also drive increasing spend optimization, gaining tighter control over the ways that employees use corporate funds.

In parallel to this, all three lines of defense can work together to rearchitect a shared internal process. Over six to nine months, the organization can gradually shift away from prior methodologies towards optimal processes, gaining more proficiency and comfort in the new way to monitor programs and influence optimized organizational spending.