

Effective Compliance

Right-Sizing Your Program

Lewis Ziropiannis

Ryan Ward

CONFIDENTIAL

© Copyright Baker Botts 2023. All Rights Reserved.



Today's Presenters

Lewis Ziropiannis, Dallas Partner



Lewis is routinely engaged to provide clients with practical and efficient solutions to complex litigation, compliance, investigation and enforcement matters across a wide range of subject matter areas and industries including financial services, technology, energy, transportation and healthcare. In addition to his federal clerkship and top-tier private practice experience, Lewis spent 10 years in executive level in-house counsel positions at two *Fortune 50* global companies operating in the financial services, energy and technology sectors. He served as the Global Head of Anti-Corruption Compliance and Investigations at AIG, Global Chief Compliance Officer of GE EFS - GE's energy investment business, and Global Chief Compliance Officer of GE Digital - GE's technology and IIoT business. In these leadership roles, Lewis regularly interfaced with the board of directors and outside regulatory agencies and managed global compliance programs, high-stakes litigation, government and internal investigations and regulatory affairs.

Ryan Ward, Dallas Associate



Prior to joining Baker Botts, Ryan's work was largely focused on securities litigation and False Claims Act litigation, where he drafted motions in federal court, prepared witnesses for depositions, and assisted in jury testing for trial.

Ryan previously served as a judicial law clerk to Judge Jan E. DuBois of the United States District Court for the Eastern District of Pennsylvania and to Judge E. Grady Jolly of the United States Court of Appeals for the Fifth Circuit.

Overview: Compliance Program Importance

Practical Considerations

- Promotes sound and ethical business practices
- Establishes guardrails for all employees
- Can give your company a competitive advantage
- Required in certain regulated industries... (*e.g.*, Healthcare and Financial Services)
- Can be used to prevent regulatory and enforcement action

Overview: Compliance Program Importance

Department of Justice (“DOJ”) Expectations

- Effectiveness of compliance programs has been an important topic of the DOJ over the last year.
 - [Evaluation of Corporate Compliance Programs \(Updated March 2023\)](#)
- Three fundamental questions to consider:
 - Is the program **well-designed**
 - Is the program adequately **resourced and empowered** to be effective
 - Does the program **work in practice**
- DOJ asks: “whether and to what extent, the corporation’s compliance program is effective **at the time of charging decision** or resolution...” (emphasis added)
 - Mitigating your program at the time of a charging decision is not enough

Overview: Compliance Program Importance

DOJ Expectations continued..

- Evaluation of compliance program effectiveness depends on a company's **risk profile** and solutions to **mitigate** identified risks
- Factors the DOJ considers include, but are not limited to:
 - Company size
 - Industry
 - Geographic footprint
 - Regulatory landscape
- Chief Executive Officer ("CEO") and Chief Compliance Officer ("CCO") Certifications
 - prosecutors have been instructed to consider requiring CEOs and CCOs to certify that the corporate compliance program is "reasonably designed" and implemented prior to releasing the company from its obligations under a resolution agreement.

Key Takeaways

- Compliance programs have a practical, business-centric purpose.
- Compliance programs are under serious scrutiny by the DOJ and other enforcement agencies.
- Effective compliance programs require upfront analysis of company risk.
- Compliance programs must be business-specific and tailored... one size DOES NOT fit all.
- Compliance resource allocation is critical.
- Effective compliance programs require stakeholder engagement and commitment by all levels of management.

We Have Never Had An Enforcement Action... Can An Effective Compliance Program Wait?

- As a rule... the answer is a **resounding NO**.
- Recent DOJ guidance has made it clear that the government will evaluate the effectiveness of a company's compliance program **at the time of a charging decision**.
- Today, if your program is at its infancy or in need of enhancement consider the following:
 - Prioritize, prioritize, prioritize If you try to do too much at once, you will likely not get anything done.
 - Have we conducted and documented a risk assessment recently?
 - Have you identified your key risks?
 - Have you engaged with senior and mid-level management regarding these risks?
 - Do you have any evidence demonstrating tone from the top?
 - Do we have written policies and procedures addressing key risks?
 - Do you have mechanisms in place for employees to raise concerns?
 - Do you have a program in place to investigate employee concerns?

My Company is Private – Aren't Compliance Programs Only for Public Companies?

- It is a misconception that only public companies must maintain an effective compliance program.
- There is nothing in the DOJ's Evaluation of Corporate Compliance Programs, or any other guidance on compliance programs which limits compliance programs to public companies.
 - For example, the Foreign Corrupt Practices Act ("FCPA") applies to "domestic concerns." A domestic concern is any individual who is a citizen, national, or resident of the United States, or any **corporation, partnership, association, joint stock company, business trust, unincorporated organization, or sole proprietorship that is organized under the laws of the United States or its states, territories, possessions, or commonwealths or that has its principal place of business in the United States.**
- A company's status as a private entity is not a defense to an ineffective compliance program.

Who Is Responsible for Compliance?

- Compliance is not the sole responsibility of the Compliance and/or Legal Departments.
- Every employee in the organization, including senior management is responsible for compliance
- The DOJ's March 2023 update to Evaluation of Corporate Compliance Programs explicitly states:
 - “[I]t is important for a company to create and foster a culture of ethics and compliance with law at all levels of the company”
 - “The effectiveness of a compliance program requires a high-level commitment by company leadership to implement a culture of compliance from the middle and the top.”
- A company's board of directors and executives set the tone
- Senior management should clearly articulate the company's ethical standards
- Middle management should reinforce these standards and encourage all employees to abide by these standards

My Resources Are Limited... What Now?

- As a practical matter... anyone sitting in a compliance leader role will likely wish for additional resources
- As risk assessment is the best tool in your arsenal to identify risks and allocate limited resources.
- No matter how limited your resources are, companies should consider the following:
 - Does personnel in the compliance function have sufficient seniority and autonomy from management such as access to the BoD and audit committee
 - Does the company have a dedicated compliance officer, who is dedicated to the compliance function
 - Does the compliance function have appropriate stature and involved in strategic and operational decisions of the company
 - Does the compliance function have access to data to assess risks associated with policy breaches and transactions
 - Does the company have systems in place to establish incentives for compliance and disincentives for non-compliance

Do I Need to Do a Risk Assessment?

- Yes! A risk assessment is the starting point in any program development or enhancement
- Factors to consider:
 - Location of operations
 - Industry
 - Market competition
 - Regulatory landscape
 - Potential clients and business partners
 - Interactions with foreign government officials
 - Whether compliance program has been tailored to risk assessment
- Risk Assessment Process and Methodology
 - Data collected
 - Metrics used
 - Documentation of Process

Do I Need to Do a Risk Assessment?

Continued...

- Resource Allocation
 - Risk assessment used to establish appropriate resource allocation
 - Are you spending disproportionate amount of time on low risks
- Is the risk assessment static or revised as needed?
 - Is the assessment only a snapshot in time?
 - Are risks reviewed periodically and risk assessment revised
 - M&A
 - New product introduction
 - New geography
 - New regulations or law changes
- Does the risk assessment account for “lessons learned” and prior compliance issues reported or faced by the company

Do We Need Written Policies and Procedures?

- Yes. Starting with a Code of Conduct:
 - Commitment to full compliance with applicable laws
 - Endorsed by Senior Leadership
 - Available and easily accessible to all employees (intranet site, onboard training, period training)
- Yes. Written policies and procedures to incorporate compliance in day-to-day operations.
 - Policies accessible, comprehensive and easy to read and understand. Avoid sweeping legal statements and standards.
 - Have policies been translated, as appropriate, for foreign subsidiaries.
 - Not a “paper compliance program.” Even if policies exist in written form, can you demonstrate they have been rolled out and implemented across the appropriate business lines and functions.
 - Have policy “gatekeepers” been assigned to verify that policies are up to date. Do these gatekeepers know what misconduct to look out for and how to escalate potential concerns to the Compliance Function

Training and Communication Tips

- Compliance training and communication should be tailored to the audience size, sophistication and subject matter expertise.
 - The training and communication program for lawyers and executives may differ from the program designed for sales representatives or factory workers
- Training and communication plans may vary:
 - Practical case studies designed to assist employees to mitigate risks
 - Short targeted training sessions designed to inform employees how to identify and raise concerns
 - Plans tailored to job function and responsibility
 - Avoid long “legal” training sessions that overwhelm audiences with legal doctrine and are ineffective in keeping attention
- Document training plan rationale
 - Training in person or virtual?
 - Who receives particular training and why
 - Consequences for failing to attend training

Training and Communication Tips

Continued...

- Does the training provide a mechanism for employees to raise questions or concerns,
- Is there a way to measure feedback or effectiveness of the training program.
- Is Senior Management engaged in communicating the importance of compliance training and integration into the business operations
- Do you publish sanitized case studies of employee misconduct and consequences for employee misconduct

Does the Compliance Program Work?

- Remember... no matter how effective, no compliance program can prevent all misconduct by all employees!
- To be effective, it is important to document that the program identified misconduct, wrongdoing was appropriately investigated and remediated.
- In addition, effective programs allow for continuous improvement, testing and review
 - Has the program been audited and what types of audits were conducted
 - Have compliance gaps been documented and reported to management and the board as appropriate
 - Have controls been tested. Has a gap analysis and remediation plan been conducted and documented
 - Does the company monitor changes in the legal and regulatory landscape
 - Does the company renew its risk assessment to evolve with business and regulatory changes
- Does the company effectively investigate wrongdoing

What is the Role of Data in Compliance?

- Data can be a powerful tool in designing and implementing your compliance program and developing your risk assessment.
- DOJ increased focus on data... in 2022 hired a new Counsel, Compliance & Data Analytics position in the Fraud Section of the Criminal Division.
- March 2023 Update to DOJ Evaluation of a Corporate Compliance Program:
 - “Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring...”
- What data sources does your company maintain? Start with low hanging fruit:
 - High risk customers and partners
 - Sanctions escalation and clearing data
 - Investigation closure rates
 - Expense reimbursement and T&E requests
 - Training metrics
 - Audit findings and closure statistics

Additional Considerations... On the Horizon

- Compliance program updates that tie compliance to compensation incentives and deterrents including financial penalty consequences for employee misconduct.
 - Prohibition on bonuses for employees who fail to adhere to compliance guidelines
 - Supervisory responsibility for managers who knew or were “willfully blind” to employee misconduct
- Implementation of risk-based policies for the use of personal devices and messaging applications to ensure preservation of business data.
 - Enforcement of preservation and access policies consistently and imposes consequences for employees who refuse to grant access
 - Whether a company “Bring Your Own Device Program” ensures data preservation
 - Access to third party messaging apps, whether stored on corporate devices or company servers

AUSTIN

BRUSSELS

DALLAS

DUBAI

HOUSTON

LONDON

NEW YORK

PALO ALTO

RIYADH

SAN FRANCISCO

SINGAPORE

WASHINGTON

[bakerbotts.com](https://www.bakerbotts.com)

©Baker Botts L.L.P., 2023. Unauthorized use and/or duplication of this material without express and written permission from Baker Botts L.L.P. is strictly prohibited. Excerpts and links may be used, provided that full and clear credit is given with appropriate and specific direction to the original content.