Developing a Legal Compliance Program

by Practical Law Commercial Transactions

Maintained • USA (National/Federal)

Related Content

This Practice Note discusses the key points to consider when developing, implementing, and maintaining a legal compliance program. Topics addressed include tone from the top, the role of chief compliance officer, coordination of internal resources, geographic and cultural challenges, risk assessment, hallmarks of an effective program, integration of mergers and acquisitions, and program documentation.

Business organizations today operate under an increasingly complex array of laws and regulations both inside and outside the US, including anti-corruption, antitrust, securities, fraud, data privacy, data security, environmental, and employment laws. A robust compliance program can be the most effective way to:

- Navigate this complicated legal environment.
- Protect the business.
- Reduce the costs associated with violations of law.

A legal compliance program brings together an organization's policies, procedures, and other compliance efforts. It should be reasonably designed, implemented, and enforced so that in general, it effectively:

- Prevents and detects violations of laws, regulations, and policies.
- Promotes an organizational culture that encourages ethical conduct and commitment to compliance with the law.
- Addresses the specific risks of an organization with concrete actions to reduce or eliminate those risks.
- Ensures that employees understand and comply with the laws, regulations, and policies that apply to their daily work.

This Note examines:

- The preliminary steps to developing an effective compliance program.
- The hallmarks of an effective program.
- Additional steps that help make the program effective.

While this Note focuses on US regulatory guidance, many of the steps and issues discussed also apply to compliance programs for multinational companies. For additional regulatory issues to address when rolling out programs outside the US, see Financial and Business Crime: Country Q&A Tool.

Preliminary Steps to Developing an Effective Compliance Program

The company and its counsel should lay the groundwork for developing a legal compliance program by taking several preliminary steps.

Obtain Top Level Commitment and Support

Executive commitment and support are vital to the successful development of an ethical culture and effective compliance program. Top level support is also a hallmark of an effective program under the **Federal Sentencing Guidelines** (Sentencing Guidelines) of the US Sentencing Commission (U.S. Sentencing Guidelines § 8B2.1(b)(1)) (see One: Strong Organizational Leadership and Ethical Culture). The company's governing body (such as its **board of directors** or board of **managers**) and senior management should:

- Provide strong, explicit, and visible support for the company's compliance program and code of conduct.
- Give the compliance program sufficient stature and political support within the company.
- Instill a culture of integrity that starts at the top (tone from the top) by consistently modeling the company's ethical values and actively communicating that everyone has ownership and responsibility for doing the right thing.
- Emphasize the vital role that compliance plays and the value that it adds to the company's performance and success (for example, by enabling cost reductions and contributing to strategic planning).

Appoint a Chief Compliance Officer

The Sentencing Guidelines require the company to appoint a person with sufficient authority to oversee the compliance program. The company should:

- Create the role of chief compliance officer (CCO) to provide the required oversight.
- Select a high-level individual to fill the role.
- Determine where the role should reside within the organization.

Determine the Organizational Structure for the CCO Role

The three most commonly selected organizational structures for the CCO are:

- The general counsel (GC) is appointed CCO and serves dual roles as both GC and CCO.
- The CCO is a separate individual but reports to the GC.
- The CCO is independent of the GC and reports directly to the chief executive officer (CEO) and the governing body.

Government authorities, including the US **Department of Justice** (DOJ), recommend that the CCO be an independent, stand-alone function, but have not explicitly required that structure. The DOJ has instead stated that it looks for evidence that a company's compliance function operates independently and with autonomy when conducting an investigation. This flexibility allows a company to tailor its compliance function to its circumstances. When selecting an organizational structure for the CCO role, the company should consider and compare the issues outlined in the table below.

Structure	Advantages of Structure	Disadvantages of Structure
The GC serves dual roles as both GC and CCO.	• The GC, as a high-level officer, meets the Sentencing Guidelines requirement for a person with sufficient authority to serve in this function. • Combining the positions can promote operational efficiency. Most compliance issues also have legal implications for the company, so the GC and CCO functions often overlap. • Placing the GC in this dual role avoids the cost of additional headcount. The Sentencing Guidelines recognize that smaller organizations may not have the resources to create a new position and may need to use existing officers to manage the compliance program.	• Having a single person serve as the GC and CCO may create a conflict of interest. While the GC's role is to defend against claims of non-compliance, the CCO's role is to ensure compliance. These can be conflicting obligations. • There are limitations on the amount of time and resources that the GC can devote to an additional responsibility.

	• The GC may be able to assert **attorney-client privilege** to protect the company's investigations and other compliance-related activities.	
The CCO is a separate individual but reports to the GC.	• Having the GC and CCO work closely together can result in operational efficiencies. • A dedicated CCO can ensure that compliance is given the attention it requires. • Having a separate person serve as CCO can add another perspective to the function and provide a level of checks and balances to the company's compliance reporting.	• The CCO may not have or may be perceived by regulators as not having sufficient authority to oversee the compliance program. • It fails to meet best practices if the CCO does not have direct access to the governing body. This structure creates a risk that the GC will filter the CCO's reporting of compliance issues to senior management and the governing body. • Even if the CCO is given a dotted reporting line to the governing body, in practice the CCO may feel uncomfortable circumventing the GC to make compliance reports.
The CCO is independent of the GC and reports directly to the CEO and the governing body.	• With adequate stature, budget, and support, this structure meets the requirement under the Sentencing Guidelines for a person with sufficient authority to oversee the compliance program. • The CCO has access to the governing body for reporting compliance issues as required under the Sentencing Guidelines. • The separate CCO and GC functions give the company two perspectives on whether it **should** do something as well as whether it **can**. • The separate CCO and GC functions can more effectively set up a system of checks and balances around the compliance program. • This structure minimizes the negative consequences that may arise if the GC and CCO roles have conflicting obligations.	• An additional senior position may be a significant cost for the company.

Create Parameters for the CCO Role

To ensure that the selected organizational structure is effective, minimizes conflicts, and facilitates the governing body's ability to oversee the company's compliance program, the company should also consider:

- Conducting periodic third-party audits of the compliance program structure under the direction of the governing body.
- If the GC and CCO are dual roles held by the same person:
  - periodically reviewing the pros and cons of this dual function in light of regulatory developments and evolving industry best practices; and
  - adopting a process for the GC to recuse itself from a compliance investigation if the matter involves the conduct or judgment of the GC or the GC's office.
- Where the GC and CCO positions are separate:
  - clarifying the job descriptions for the two positions to minimize overlap and conflict;
  - assuring appropriate peer-level status between the two functions; and
  - creating effective communications processes between the two roles to promote operational efficiency and coordination.

Coordinate Internal Resources

Companies typically have pockets of compliance initiatives led by separate departments and groups across the organization (for example, legal, human resources, **audit committee**, accounting, and information technology). While the risks may overlap or interrelate, these compliance activities are often uncoordinated. As a result, compliance initiatives may be planned and managed in parallel silos, which can increase the overall risk and cost for the company. When developing its legal compliance program, the company should eliminate this inefficiency and duplication by first:

- Identifying the business functions and processes in the company that already play a role in maintaining compliance.
- Determining if any additional roles may be relevant to the regulations, statutes, and other requirements applicable to the company.
- Collaborating with all of these roles to align compliance standards, processes, and procedures.

By determining which employees are key stakeholders, the company can take steps to:

- **Engage employee stakeholders early in the process.** The company should develop an interactive communication plan to share program information and gather stakeholder feedback. This step:
  - gives employee stakeholders a sense of involvement in and ownership of the compliance program;
  - educates them about the goals and benefits of the program, why particular compliance policies and processes are being considered, and how the program may affect their functions; and
  - allows the company to gain valuable insight into the operational needs and concerns within the organization and to use this information to build a more robust program.
- **Obtain employee stakeholder buy-in and support.** For a compliance program to be effective, a company may need to undergo organizational changes and cultural shifts. Deliberate engagement of employee stakeholders can help the company obtain the stakeholder buy-in and support needed to bring about these changes.
- **Assemble an internal team of compliance champions.** The use of compliance champions helps the company leverage internal resources to increase the impact of its compliance function. It can also foster employee commitment to compliance by encouraging the participation of individuals who are not necessarily attorneys or compliance professionals. Compliance champions can be given important tasks to help the program gain traction, build momentum, and reach objectives. For example, the company may consider using compliance champions to:
  - convey positive messages about the compliance program and encourage cooperation from their peers and teams;
  - support employee transition to a new compliance environment;
  - serve as the initial point of contact for compliance questions in their communities or groups;
  - train local employees on compliance processes; and
  - funnel innovative program ideas and other feedback from the workforce.

  This internal team should consist of representatives from across the organization, such as legal, compliance, internal audit, risk management, human resources, information technology, finance, accounting, investor relations, marketing, sales, and other relevant groups.

Consider Geographic Scope and Cultural Differences

The company may face different compliance challenges depending on the geographic areas that are relevant to its business. The company should determine its geographic scope by identifying where its:

- Business operations and employees are located.
- Materials are sourced.
- Suppliers and customers do business.
- Key business partners operate.

To develop a compliance program that is effective in the local context, the company should consider:

- Researching industry developments and competitor responses to compliance issues in the relevant geographic areas to better understand the specific challenges in those areas and possible approaches to those issues.
- Obtaining feedback from applicable stakeholders in the field on how to bridge geographic divides and cultural gaps.
- Incorporating practical steps and specific examples and advice that make the program relevant to the local audience (for example, by changing training hypotheticals to use examples from the local business).
- Communicating compliance policies and procedures in a variety of styles (for example, with local language translations, interactive exercises, and online and live presentations) to encourage cultural acceptance and understanding by local employees and business partners.
- Identifying and addressing other cultural sensitivities that affect how the company implements the program. For example, in certain cultures, a hotline may carry negative connotations as a snitch line. In those locations, the company may want to promote acceptance of its hotline by naming it a helpline or guideline (see Setting Up and Operating a Company Hotline Checklist: Understand Local Laws and Culture and Article, Whistleblowing: New risks, new responses: Naming the hotline and Local considerations).

Conduct an Initial Risk Assessment

The risk assessment focuses the company's governing body and senior management on the most significant risks within the organization. It provides the basis for allocating resources to avoid, mitigate, or remediate those risks. The company's counsel and CCO should partner with the internal audit function or engage external resources to:

- Gather information to understand and analyze the organization's enterprise-wide business activities.
- Thoroughly review the regulatory and contractual requirements applicable to the business.
- Create a risk profile or risk matrix that:
  - identifies potential legal risks within the organization;
  - determines the owners of those risks and the controls already in place for them;
  - assesses the level of risk for each risk area;
  - prioritizes the likelihood of a violation; and
  - quantifies the likely damage to the organization from a violation.

For example, for resources to help collect information and guidance on conducting:

- An antitrust risk assessment, see Standard Document, Antitrust Merger Analysis Information Request: Manufacturing.
- A bribery risk assessment, see Standard Document, Anti-Bribery Third-Party Risk Assessment: Business Unit Questionnaire.
- A data security risk assessment, see Practice Note, Data Security Risk Assessments and Reporting and Performing Data Security Risk Assessments Checklist.
- A privacy compliance audit and risk assessment, see Standard Document, Privacy Audit Questionnaire.

Address Key Risks

Once the company has identified its key risks, it should design its compliance strategies to address those risks. In addition to the following common risk areas, the company may also need to address particular risks that are specific to its organization or industry.

Advertising and Marketing Risks

Various laws and regulations apply to advertising and marketing practices, such as laws dealing with:

- Misleading advertisements (see Practice Note, Advertising: Overview: False or Misleading Advertising).
- Comparative advertising (see Practice Note, Comparative Advertising Law in the US).
- Advertising to children (see Practice Note, Children's Online Privacy: COPPA Compliance).

- Promotions, including contests and sweepstakes (see Promotions Toolkit).

For resources to help the company structure its advertising and marketing campaigns to comply with consumer protection laws and industry best practices, see Advertising and Marketing Toolkit.

Anti-Bribery and Foreign Corrupt Practices Act Risks

Anti-corruption compliance has become an increasingly important area of risk management for companies transacting business internationally. For resources to help the company understand anti-corruption laws, including the US **Foreign Corrupt Practices Act of 1977** (FCPA) and the UK **Bribery Act 2010**, and implement effective anti-bribery compliance measures (such as internal controls for accurate books and records), see Bribery and Corruption Toolkit.

Antitrust and Competition Risks

High-risk activities that may result in antitrust violations include:

- Price-fixing (see Practice Note, Pricing Strategies and Antitrust: Price-Fixing).
- Market or customer allocations (see Practice Note, US Antitrust Laws: Overview: Horizontal or Vertical Restraints).
- **Exclusive dealing** (see Practice Note, Exclusive Dealing Arrangements and Exclusive Dealing Antitrust Risk Factors Checklist).
- **Predatory pricing** (see Practice Note, Customer Loyalty Programs in the US: Legal Elements of Predatory Pricing).
- **Tying arrangements** (see Practice Note, Tying Arrangements).
- **Resale price maintenance agreements** (see Practice Note, Pricing Strategies and Antitrust: Resale Price Maintenance and Its Alternatives and Resale Price Maintenance Under State Laws Chart).

For resources to help the company conduct an antitrust audit and implement antitrust compliance measures, see Antitrust Compliance Toolkit.

Data Privacy and Data Security Risks

Companies must pay close attention to the patchwork of state, federal, and foreign laws governing the collection, use, transfer, disposal, and security of **personal information**. A company should address end-user privacy considerations when collecting personal information and implement appropriate administrative, technical, and physical safeguards to protect personal information. For a sample internal privacy policy, see Standard Document, Personal Information Protection Policy (Internal).

For more resources to help the company create, set up, and review the company's privacy and data security compliance programs, see:

- Practice Note, Developing a Privacy Compliance Program.
- Privacy Compliance and Policies Toolkit.
- Data Breach Toolkit.
- Information Security Toolkit.

Employee Benefits Risks

Failure to comply with the many laws, rules, and regulations governing employee benefits can result in significant risk to a company, including excise taxes and participant claims for lost benefits. The company should have a strategy for implementing a compliant employee benefits program, including:

- Complying with the **Employee Retirement Income Security Act of 1974** (ERISA) (see, for example, SPD Compliance Chart for ERISA Plans and ERISA Litigation Toolkit).
- Satisfying obligations under the **Affordable Care Act** (ACA) (see Affordable Care Act (ACA) Toolkit and Employer Mandate Toolkit) and other rules applicable to **group health plans** (see Group Health Plans Toolkit).
- Meeting **qualified plan** requirements (see Practice Note, Requirements for Qualified Retirement Plans and Qualified Retirement Plan Provisions Toolkit).
- Addressing related plan design issues. For more information, see:

- Practice Note, Defined Contribution Health Plans: Overview.
- Practice Note, Voluntary Benefits.
- Fringe Benefits Toolkit.

For an overview of the key issues and laws that apply to employee benefits, including the **Internal Revenue Code** (Code) and ERISA, see Practice Note, Employee Benefits Law: Overview.

Employment Risks

Given the sheer volume of federal, state, and local labor and employment laws, employment-related claims are one of the most significant areas of legal exposure for a company. The company should take steps to minimize employment-related risk, particularly in the areas of:

- **Harassment** and discrimination claims, including:
  - sexual harassment claims (see Sexual Harassment Toolkit);
  - charges filed with the **Equal Employment Opportunity Commission** (EEOC) (see Preventing and Responding to Discrimination Complaints Checklist and Preventing and Responding to an EEOC Charge Toolkit);
  - discrimination claims under state law (see Anti-Discrimination Laws: State Q&A Tool); and
  - **retaliation** claims (see Practice Note, Retaliation).
- Other claims under **Title VII of the Civil Rights Act of 1964** (Title VII), such as claims relating to religious discrimination and accommodation (see Practice Notes, Discrimination Under Title VII: Basics and Religious Discrimination and Accommodation Under Title VII).
- **Disability** discrimination and accommodation (see Practice Notes, Disability Discrimination Under the ADA and Disability Accommodation Under the ADA).
- Age discrimination (see Practice Note, Age Discrimination).
- Leave laws (see Employee Leave Toolkit).
- **Independent contractor** classification (see Independent Contractor Toolkit).
- Wage and hour compliance (see Practice Note, Conducting an Internal Wage and Hour Audit and Wage and Hour Claims Toolkit).
- **Trade secret** and confidential information protection (see Practice Note, Protection of Employers' Trade Secrets and Confidential Information and Trade Secrets and Confidential Information Best Practices at Hiring Checklist).
- Immigration (see Practice Notes, Demonstrating the Right to Work in the United States and Employer Obligations Under State Immigration Laws in the US).
- Health and safety in the workplace (see Practice Note, Health and Safety in the Workplace: Overview, Employer Compliance with the Occupational Safety and Health Act Checklist, and Minimizing Workplace Violence Checklist).

For general resources to help the company assess its human resources practices, see Human Resources Audit Toolkit.

Environmental Risks

A company may have potential environmental liabilities and exposures even if its business does not directly involve hazardous materials. For example, in a commercial real estate transaction, the parties often perform environmental due diligence to identify any environmental concerns relating to the properties involved in the transaction. For more information on environmental due diligence, see:

- Practice Note, Commercial Real Estate Loans: Environmental Due Diligence for Lenders.
- Practice Note, Purchaser Due Diligence in Commercial Real Estate Acquisitions: Environmental Issues.
- Standard Document, Due Diligence Request List (Commercial Real Estate).

For an overview of the environmental regulatory framework and the major environmental statutes that impact businesses, as well as the types of liability imposed on violators of these laws and regulations, see Practice Note, Environmental Law: Overview.

Intellectual Property (IP) Risks

Various IP risks may arise during the course of a company's operations and business transactions. A company often must protect and manage its own IP rights as well as identify and minimize the risk of infringing third-party IP rights.

For more information on IP risks involving infringement claims, see Practice Notes:

- Copyright Infringement Claims, Remedies, and Defenses.
- Trademark Infringement and Dilution Claims, Remedies, and Defenses.
- Patent Infringement Claims and Defenses.

For more information on IP risks involving the protection and management of a company's IP assets, see:

- Practice Note, Patent Portfolio Development and Management.
- Trademark Registration and Maintenance Toolkit.
- Brand Protection Toolkit.

Internet and Email Risks

Companies rely on online media and communications technologies both in their interactions with customers, suppliers, and other third parties and in their internal operations and communications. For resources to help the company identify, manage, and mitigate the risks associated with the operation and use of websites, email, and other online media technology and applications, see:

- Internet and Email Risk Toolkit.
- Social Media Usage Toolkit.
- Internet, Mobile, and Marketing Privacy Compliance Toolkit.

Securities and Corporate Governance Risks

Public companies face additional risks relating to, for example:

- Specific reporting and disclosure obligations (see New Public Company Toolkit (Domestic Issuers) and New Public Company Toolkit (Foreign Private Issuers)).
- **Insider trading** (see Standard Document, Corporate Policy on Insider Trading).
- Accounting fraud (see Practice Note, Trends in Federal White Collar Prosecutions: Accounting Fraud and Obstruction of Justice).
- The misrepresentation or omission of material information (see Standard Document, Memorandum: Internal Reporting Procedures for Material Events, Potentially Triggering Form 8-K Filings and Is it Material? Asking the Right Questions Checklist).

For information on US federal securities law requirements and corporate governance standards, see Practice Notes:

- US Securities Laws: Overview.
- Internal Control Over Financial Reporting for Counsel: Why Should You Care?.
- Corporate Governance Standards: Overview.
- Periodic Reporting and Disclosure Obligations: Overview.

Trade Compliance Risks

Before conducting an international transaction, including the import and export of goods and services, the company should verify if the transaction or the underlying conduct complies with applicable law. In particular, the company should be mindful of the risks relating to:

- Trade restrictions, export controls, anti-boycott laws, **tariffs**, non-tariff trade barriers, and customs-related issues (see International Trade Toolkit).
- Corporate social responsibility trends affecting the supply chain (see Corporate Social Responsibility Toolkit).
- **Conflict minerals** disclosure rules that apply to public companies (see Conflict Minerals Rule Compliance Toolkit).

For resources to help the company develop import and export compliance programs, see:

- Practice Note, Core Elements of an Import Compliance Program.
- Practice Note, Core Elements of an Export Compliance Program.
- Standard Document, Import Compliance Policy.
- Standard Document, Statement of US Export and Trade Compliance Policy.

Organization-Specific Risks

The company may face additional risks relating to the:

- **Specific countries in which it operates.** For example, when doing business in countries such as Argentina, Venezuela, Bolivia, and Russia, the risk of **expropriation** is viewed as greater because these governments have acquired control of all or part of foreign companies in recent years (see Practice Note, Political Risk Insurance: Is it Necessary?: Location of the Project). For general considerations when doing business outside the US, see Doing Business in…Country Q&A Tool.
- **Government interactions that occur in its business.** For example, interactions with foreign governments to obtain permits or approvals and conduct other business transactions often increase the corruption risk (see Practice Note, The Foreign Corrupt Practices Act: Overview: Recognizing Red Flags).
- **Nature and types of transactions it undertakes.** For example, for companies that engage in:
  - cross-border transactions with related entities, transfer pricing is a key risk (see Practice Note, US Transfer Pricing: Managing Risks);
  - project finance transactions, typical risks include construction risk, operational risk, offtake risk, and **political risk** (see Practice Note, Identifying and Managing Project Finance Risks and Standard Document, Project Finance Risk Matrix); and
  - commercial contracts, consideration should be given to common risk allocation mechanisms, such as **indemnification**, limitations on liability, termination rights, **force majeure**, insurance coverage, and other contractual remedies (see Practice Note, Risk Allocation in Commercial Contracts and Insurance Policies and Coverage Toolkit).
- **Joint ventures and other business partnerships it considers.** Risks may include:
  - conflicts of interest;
  - third-party liability;
  - breach of contract; and
  - other disputes among the strategic partners.

  (See Minimizing Risk in US Strategic Alliance Transactions Checklist and Joint Ventures Toolkit.)

Industry-Specific Risks

There may be industry-specific risks that affect all companies within that industry. There may also be industry-specific requirements for the company to comply with accepted standards and applicable law. For example, companies in the:

- Food, cosmetic, and other industries may face specific risks relating to labeling requirements. For more information, see Practice Notes:
  - Product Labeling;
  - Food Product Labeling;
  - FDA Cosmetic Labeling Regulations; and
  - FTC Labeling Requirements for Consumer Goods.
- Tobacco, alcohol, and financial and consumer credit industries must comply with specific advertising regulations (see Practice Note, Advertising Overview: Industry-Specific Regulation).
- Manufacturing sector have greater exposure to product liability risk (see Practice Notes, Product Liability Claims, Defenses, and Remedies and Preempting and Mitigating Product Liability Claims).

- Banking and financial services sector must comply with requirements for, among others:
  - anti-money laundering (see Practice Note, US Anti-Money Laundering and Trade Sanctions Rules for Financial Institutions);
  - privacy and data security (see Financial Privacy Compliance Toolkit); and
  - know-your-customer or customer identification obligations (see Practice Note, USA PATRIOT ACT and Know Your Customer Requirements for Lenders).
- Healthcare sector generally must comply with the **Health Insurance Portability and Accountability Act of 1996** (HIPAA) (see HIPAA Privacy, Security, and Breach Notification Toolkit).

For categories of industry-specific risk factors commonly included in offering documents and periodic reports filed with the **Securities and Exchange Commission** (SEC), see Practice Note, Risk Factors: What Keeps You Up at Night?: Industry Risk Factors.

Ten Hallmarks of an Effective Compliance Program

The Sentencing Guidelines, together with additional guidance provided by the DOJ, form the cornerstone of a company's legal compliance program. They identify the hallmarks or core elements generally considered by regulators to be the minimum requirements for an effective program (see U.S. Sentencing Guidelines § 8B2.1(b)(1)). Once the company has identified its key risks (see Conduct an Initial Risk Assessment and Address Key Risks), it should address those risks by adapting and implementing the core elements to fit its particular needs and circumstances. Ongoing identification, adaptation, and implementation are part of the iterative process that characterizes an effective compliance program.

One: Strong Organizational Leadership and Ethical Culture

The company's governing body, senior management, and managers and supervisors must play key roles in developing and implementing an effective legal compliance program. All members of leadership should:

- Promote a culture that encourages ethical conduct and compliance.
- Be knowledgeable about the content and operation of the program.
- Visibly support the program.

The Governing Body

The company's governing body should be accountable for the program (see Obtain Top Level Commitment and Support). It should have the knowledge and experience to understand and effectively oversee the program, though its level of technical knowledge and experience may vary depending on the particular circumstances at the organization. Specifically, the governing body is responsible for:

- **Staying informed of compliance risks.** The governing body should:
  - obtain practical management information about the company's compliance risks; and
  - be aware of compliance risks that other companies within its industry or with similar operations face.

  (See Practice Note, Corporate Governance Practices: Commentary: Risk Management.)
- **Approving the program.** The governing body should review and approve the key elements of the compliance program, including:
  - policies;
  - risk management standards; and
  - roles and responsibilities of committees and functions with compliance oversight responsibilities.

  This review should include an evaluation of whether the primary program features are adequate to address the company's key risks.
- **Empowering the CCO.** The CCO should:
  - have adequate autonomy from senior management to perform the job; and
  - be given direct access to the governing body to report on the status of compliance throughout the organization.

- **Providing feedback on the program.** The governing body should:
  - assess the effectiveness of the program;
  - review the company's responses (such as discipline and corrective measures) when compliance problems are detected; and
  - provide appropriate input and feedback to the CCO.
- **Holding management accountable for program results.** Senior management should be fully capable and properly motivated to manage the company's compliance risks, consistent with the governing body's expectations (see Six: Incentives and Discipline to Promote and Enforce Compliance).

For a discussion of the board's role in overseeing and assessing the company's compliance program, see Article, Board Assessment of Compliance Programs.

Senior Management

Like the company's governing body, senior management is also responsible for overseeing the compliance program and setting the proper tone from the top (see Obtain Top Level Commitment and Support). In addition, senior management is responsible for:

- **Communicating the importance of compliance.** Senior management should reinforce this message across all levels of the organization and implement measures to promote a culture of compliance.
- **Empowering the CCO.** The CCO and any senior compliance personnel within individual business lines should have appropriate authority and independence to implement the program and drive meaningful change.
- **Allocating resources to the program.** The CCO should have adequate funding and appropriate resources (for example, technology for automated controls, and tracking and reporting tools) to effectively develop and operate the compliance program. In allocating resources, senior management should take into account the organization's size, risk, resources, and scope of the compliance program.
- **Partnering with the CCO and managing operational changes.** Senior management should cooperate with the CCO and manage the changes needed within the organization to implement the program and comply with compliance policy requirements.
- **Providing feedback on the program.** Senior management should review the CCO's compliance status reports and provide appropriate feedback on the effectiveness of the program.
- **Holding managers and employees accountable for compliance.** Senior management should set appropriate accountability measures and incentives to integrate compliance initiatives (such as mandatory training requirements) into:
  - management and employee goals;
  - performance evaluations; and
  - the compensation structure across the organization.

  (See Six: Incentives and Discipline to Promote and Enforce Compliance.)

Managers and Supervisors

All managers and supervisors should be knowledgeable about the compliance program and echo the tone from the top. While the company needs its leadership to value compliance from the top down, it also needs to foster compliance from the bottom up. An effective compliance program requires a supportive tone in the middle so that the compliance message permeates communications and employee relations at all levels in the company.

Two: Standards and Procedures for an Effective Program

An effective legal compliance program requires standards of conduct and internal controls and procedures that are reasonably effective in reducing the likelihood of misconduct. In determining the appropriate actions to take and standards to set, the company should consider:

- The standards required by applicable government regulation.
- Industry practice.
- The size of the organization. A large organization generally should devote more formal operations and greater resources to its compliance program than a small organization.

- Similar misconduct. An organization should be extra vigilant in areas where misconduct has previously occurred. Recurrence of similar misconduct (for example, fraud) creates doubt as to the effectiveness of the compliance program.

Minimum Program Standards

At a minimum, the company should:

- **Develop a strong code of conduct and ethics.** This code should:
  - include a statement of organizational values from the company's top executive (such as the CEO, president, executive director, or equivalent role);
  - define the culture and expected behavior within the organization; and
  - for public companies listed on the **New York Stock Exchange** or **NASDAQ Stock Market**, follow **Sarbanes-Oxley Act of 2002** (SOX) requirements relating to codes of ethics and corresponding requirements adopted by the applicable securities exchange (see Practice Note, Corporate Governance Standards: Code of Ethics or Conduct and Standard Document, Code of Ethics and Business Conduct for a Public Company).
- **Prepare an employee handbook and other written policies and procedures.** The handbook and policies guide the company's directors, officers, and employees in performing their respective responsibilities. For resources to help counsel:
  - create, maintain, and distribute employee handbooks, see Employee Handbook Toolkit;
  - understand a range of compliance-related topics and create materials that comply with applicable law, see In-House Compliance Center; and
  - prepare compliance policies addressing different risk areas, see the collection of sample policies in the In-House Company Policies Center.
- **Extend its compliance program to all of its subsidiaries.** The program should be implemented throughout the organization and include group entities in non-US jurisdictions. In reaching its non-US entities, the company should:
  - review the risks that are specific to the organization's relevant geographic areas and create a plan to address those risks within the context of the overall compliance program (see Conduct an Initial Risk Assessment); and
  - translate its code of conduct and other written policies and procedures, as appropriate, into local languages for employees to understand (see Consider Geographic Scope and Cultural Differences).
- **Implement financial and accounting controls.** The company should ensure the maintenance of fair and accurate books, records, and accounts to comply with applicable laws and regulations, loan covenants, and other contractual obligations. For example, under the accounting provisions of the FCPA, enforcement agencies view accurate books and records as a check against corrupt payments (see Practice Note, The Foreign Corrupt Practices Act: Overview). For more information on **internal control over financial reporting**, see Practice Note, Internal Control Over Financial Reporting for Counsel: Why Should You Care?
- **Enforce policies throughout the organization.** The company should:
  - ensure that policies are not only circulated but also well-communicated and properly administered throughout the organization; and
  - clearly announce and enforce its expectation that all directors, officers, and employees follow company policies.

Three: Oversight, Autonomy, and Resources for the Compliance Function

The CCO should have the formal authority, access to leadership, resources, and respect needed to manage and implement the program.

Responsibilities of the CCO

The CCO is responsible for:

- **Developing the program.** The CCO should develop an effective and efficient compliance program for approval and adoption by the company's governing body. In presenting and advocating for the program, the CCO should:
  - set expectations for the governing body and senior management;
  - develop substantive metrics and milestones;

- create a multi-year plan for the program; and
- coordinate with the internal team of compliance champions to promote and support the program throughout the company.

- **Coordinating risk assessments.** Enterprise-wide initial and periodic risk assessments help the company identify compliance risk throughout its operations (see Conduct an Initial Risk Assessment and Ten: Ongoing Risk Assessment to Maintain Program Effectiveness).
- **Implementing compliance policies.** The CCO should ensure that these policies are communicated to employees, implemented, understood and followed, and updated as needed (see Two: Standards and Procedures for an Effective Program).
- **Conducting compliance training.** All directors, managers, and employees throughout the organization should undergo appropriate compliance training (see Four: Ongoing Training and Communication on Compliance Matters).
- **Managing reporting mechanisms.** The company should have processes and mechanisms for employees and agents, if appropriate, to report non-compliance and receive responses to their reports (see Five: Internal Reporting Mechanisms).
- **Enforcing the program.** The CCO should partner with senior management to:
  - implement compliance incentives, enforcement mechanisms, and disciplinary measures;
  - create a strategy for communicating those standards throughout the organization; and
  - tie compliance standards to functional areas within the organization that are responsible for administering discipline.

  (See Six: Incentives and Discipline to Promote and Enforce Compliance.)
- **Overseeing compliance investigations.** The CCO should coordinate with internal and external counsel, as appropriate, to determine when investigations are required and how they should be handled. This includes:
  - overseeing or conducting the investigation;
  - recommending corrective action and prevention strategies for approval by the company's governing body and senior management; and
  - confirming that corrective action has been implemented.

  (See Seven: Follow-up and Investigations of Complaints and Violations.)
- **Coordinating third-party due diligence.** The CCO should coordinate with internal counsel and business functions to:
  - understand the scope of the company's third-party relationships;
  - tailor the due diligence program to address the risks posed by those third parties; and
  - prepare and execute the company's third-party due diligence procedures.

  (See Eight: Due Diligence and Oversight of Third-Party Relationships.)
- **Overseeing compliance audits.** By reviewing the company's risk areas, the CCO and internal audit function can identify the necessary auditing and monitoring activities and set up an auditing and monitoring plan (see Nine: Monitoring and Auditing of Program Effectiveness).
- **Keeping the governing body and senior management informed.** The CCO should report at least annually (and more frequently, if appropriate, based on hotline, investigation, or auditing reports) on the status of compliance throughout the organization and other relevant compliance issues.

Build a Team of Compliance Personnel

Depending on the size of the organization, the company may designate one or more high-level personnel as compliance officers with day-to-day responsibility for the operation of the program. The company should avoid assigning compliance responsibilities to individuals who it knows or should know have engaged in illegal activities or other conduct inconsistent with an effective compliance program. As part of its process for selecting the CCO and other compliance personnel, the company should conduct due diligence on the individuals, including:

- **Background and reference checks.** For:
  - information on **background checks** on current or prospective employees, see Practice Note, Background Checks and References and Using Background Checks in Employment Checklist;
  - state-specific guidance on background checks, see Background Check Laws: State Q&A Tool; and

- a sample employee background check policy, see Standard Document, Background Check Policy.

- **Screenings against applicable government watch lists.** For example, the company should screen individuals against:
  - the database of parties excluded from federal contracts and subcontracts, maintained by the US government's System for Award Management (SAM);
  - the Debarred Parties List of persons and entities denied export privileges under the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR), published by the US Department of State's Directorate of Defense Trade Controls;
  - the Denied Persons List of persons and entities denied export privileges, published by the US Department of Commerce's Bureau of Industry and Security; and
  - the Specially Designated Nationals and Blocked Persons List (SDN) of sanctioned persons and entities with whom the company should not transact business, published by the US Department of the Treasury's **Office of Foreign Assets Control** (OFAC).

  A Consolidated Screening List of the US Departments of Commerce, State, and the Treasury is published by the US Department of Commerce's International Trade Administration. For more information on screening against denied persons lists, see Complying with US Export Control Regulations Checklist: Investigate Restricted Parties and Prohibited End Users and Restricted Party Screening Checklist.

Four: Ongoing Training and Communication on Compliance Matters

Ongoing and active training and communication are an integral part of an effective legal compliance program and one of the best strategies for a company to prevent compliance issues.

Compliance Training

To promote understanding of the company's internal standards and procedures and the requirements of external laws and regulations, the company should:

- Train its directors, officers, employees (including new employees during onboarding) and, where appropriate, agents and business partners, at least annually on:
  - the laws and policies applicable to them, including specific training on identified risk areas (for example, marketing practices or third-party payments);
  - activities prohibited under applicable laws and policies;
  - ways to recognize and report potential violations; and
  - the penalties and consequences resulting from violations.

  For a collection of presentation materials that counsel can customize and use to train the company's board of directors, business management, and other employees, see In-House Training and Guidance Center.

- Use different styles and languages to effectively present and systematically reinforce compliance training and engage training participants throughout the company's applicable geographic areas (see Consider Geographic Scope and Cultural Differences).

- Obtain annual certifications from training participants where they acknowledge training and agree to abide by company policies and applicable law. For a sample employee acknowledgment form, see Standard Documents, Training Acknowledgment and Stand-Alone Policy Acknowledgment.

- Train managers on how to properly address complaints of misconduct and avoid retaliatory actions. For sample guidelines on how supervisors should respond to employee concerns, see Standard Document, Responding to Employee Concerns: Supervisor Guidelines.

Compliance Communications

The company should also:

- Communicate often with directors, officers, employees, and, where appropriate, agents and business partners, on the program's standards and procedures and other compliance information consistent with their respective responsibilities, including:

    - incentives awarded for compliance, enforcement mechanisms used by the company, and disciplinary procedures followed when non-compliance occurs (see Six: Incentives and Discipline to Promote and Enforce Compliance); and
    - procedures for seeking guidance and reporting potential violations and questionable conduct (see Five: Internal Reporting Mechanisms).
- Repeat and reinforce the company's compliance message using multiple communication channels, such as:
    - email;
    - a compliance intranet page;
    - periodic briefings at town hall meetings;
    - short videos or other media materials displayed in the company's communal spaces;
    - discussions of compliance topics at board, staff, and sales meetings;
    - newsletters; and
    - other internal publications.
- Emphasize to directors, officers, and employees that compliance training is important and mandatory. The company should:
    - monitor training participation;
    - test comprehension; and
    - enforce training requirements.

Five: Internal Reporting Mechanisms

Reporting mechanisms are a vital part of an effective compliance program. They:

- Encourage important communication between employees and management.
- Allow employees to report sensitive matters outside the normal supervisory channels.
- Provide management with valuable information that can be used to reduce risk and liability for the company.

Create Reporting Mechanisms

The company should create multiple, convenient reporting mechanisms for employees and agents (if appropriate) to seek guidance, raise compliance concerns, and report potential or actual misconduct. These communication channels may include internal or external telephone or online hotlines and may be confidential and anonymous. When implementing a reporting mechanism, the company should consider that confidential and anonymous hotlines are:

- Required under SOX for public companies to receive reports of accounting and auditing concerns (see Practice Note, Corporate whistleblowing hotlines and EU data protection laws: US Sarbanes-Oxley Act of 2002).
- Considered best practices by regulators (such as for antitrust and FCPA compliance) (see Practice Note, Antitrust Compliance Programs: Hotline and Article, Trends in FCPA and International Anti-corruption Enforcement).
- Subject to regulatory approval and limitations in some non-US jurisdictions (see Practice Note, Corporate whistleblowing hotlines and EU data protection laws).

For a sample policy on reporting and handling whistleblower complaints, see Standard Document, Compliance Reporting Policy.

Prohibit Retaliatory Conduct

The company should assure employees that their good faith reports are protected and encouraged and can be made without fear of retribution. Retaliation against employees for reporting misconduct may be a violation of SOX and other federal and state laws. Apart from the company's risk of liability for these violations, fear of retaliation has a chilling effect on employees and severely undermines the effectiveness of any compliance program.

For more information on setting up reporting mechanisms, including hotlines, see Setting Up and Operating a Company Hotline Checklist and Article, Whistleblowing: New risks, new responses: Hotlines.

For information on whistleblower protections under state, federal, and non-US laws, see Practice Notes:

- Practice Note, Whistleblower Protections Under Sarbanes-Oxley and the Dodd-Frank Act.
- Practice Note, Whistleblower Complaints Under the ACA.
- Practice Note, Whistleblower Complaints Under the Occupational Safety and Health Act.
- Financial and Business Crime: Country Q&A Tool, Question 33.

For resources to help the company comply with whistleblower laws and minimize the risk of retaliation, see:

- Practice Note, Retaliation.
- Preventing and Responding to Retaliation Complaints Checklist.
- Standard Document, Anti-Retaliation Policy.
- Standard Document, Whistleblower Reporting: Presentation Materials.

Six: Incentives and Discipline to Promote and Enforce Compliance

The effectiveness of a company's compliance program depends on its ability to influence and guide the conduct of employees. To create this impact, the company should implement and clearly communicate incentive measures, enforcement mechanisms, and disciplinary procedures throughout the organization, including:

- **Employee job descriptions that incorporate compliance responsibilities.** Job descriptions should require employees to demonstrate and promote compliance (see Practice Note, Recruiting and Interviewing: Minimizing Legal Risk: Language of Job Descriptions).
- **Performance goals and metrics to reinforce compliant behavior.** Performance standards should be set for:
  - all senior leaders and company managers and require accountability to foster a culture of compliance; and
  - all employees to recognize and encourage compliant behavior.

  For guidance on conducting employee performance reviews, see Practice Note, Conducting Employee Performance Reviews. For a sample policy on performance reviews, see Standard Document, Performance Review Policy.
- **Incentives for meeting compliance objectives.** Rewards for employees and managers should be built into the compensation structure throughout the organization. For information on incentive-based compensation arrangements, see Standard Document, Annual Cash Bonus Plan (Designed to Comply with Section 162(m)'s Performance-Based Compensation Exception) and Section 162(m) Performance-Based Compensation Exception.
- **Clear and specific disciplinary policies for non-compliance.** Employees and managers should understand the consequences for violating the law, company policies, or compliance program requirements (such as the failure to comply with training requirements or take action when aware of non-compliance). The DOJ has specifically stated that it is unacceptable for companies to discipline low-level employees who may have implemented the bad conduct, while the senior managers who knew of or even directed the conduct are left in place. Disciplinary measures:
  - may include verbal warnings, suspensions, terminations, and financial penalties;
  - should be fair and consistent, regardless of an individual's position or status; and
  - should be appropriate and determined on a case-by-case basis, taking into account all relevant factors.

  For guidance on employee discipline, see Best Practices for Employee Discipline Checklist and Practice Note, Discipline and Discharge Under the National Labor Relations Act.
- **Internal coordination to administer discipline.** The compliance function should coordinate with other areas of the organization that have primary responsibility for administering discipline to ensure that appropriate discipline is imposed when non-compliance occurs.

Seven: Follow-up and Investigations of Complaints and Violations

An effective compliance program should include a comprehensive process for responding to reports of potential or actual non-compliance. As part of this process, the company should:

- **Stop the reported misconduct.** The company should take immediate steps to stop any misconduct. For example, with an antitrust violation, the company may need to halt transactions with third parties involved in the misconduct or, with an FCPA violation, stop a subsidiary's practice of providing gifts to government officials.
- **Prohibit retaliation against the reporter.** The company should adopt, publicize, and enforce a policy prohibiting retaliation against any employee who reports suspected compliance violations or misconduct (see Standard Document, Anti-Retaliation Policy).
- **Investigate the report.** The company should promptly and thoroughly investigate the report to:
  - verify the existence and scope of any non-compliance;
  - determine the underlying conduct that caused the non-compliance; and
  - identify all culpable individuals.

  Depending on the circumstances, the nature and type of investigation may vary and take the form of an informal inquiry, a full audit, or other review. The company should create and implement written protocols for conducting investigations. For more information on:
  - the process and management of internal investigations, see Practice Note, Internal Investigations: Whistleblower Complaints and Standard Document, Internal Investigations Policy;
  - circumstances that may necessitate a board-driven internal investigation, see Article, Board-Driven Internal Investigations; and
  - conducting internal investigations generally, see Conducting Internal Investigations: Addressing Employee Complaints and Compliance Issues Toolkit and Conducting Internal Investigations: SEC and DOJ Investigations Toolkit.
- **Cooperate with enforcement agencies.** If appropriate, the company should report the violation and investigation findings to and cooperate with the applicable government agency.
- **Take remedial action.** The company should consider remedial measures that are appropriate and adequate given the nature of the misconduct and the resulting harm. These remedial measures could include restitution to identifiable victims or termination of agreements that caused the harm.
- **Discipline wrongdoers.** The company should appropriately discipline the culpable individuals, which may include replacing any managers responsible for the misconduct (see Six: Incentives and Discipline to Promote and Enforce Compliance).
- **Prevent similar future misconduct.** The company should:
  - assess whether the violation results from any deficiencies in policies, practices, or internal controls; and
  - implement corrective measures to prevent similar misconduct in the future. For example, corrective measures may include compliance modifications, such as developing a new policy on petty cash management to minimize corrupt payments or devising a data encryption plan to counter data breaches.
- **Keep the governing body and senior management informed.** The CCO should report regularly to the company's governing body and senior management on the status and findings of investigations. For a sample investigation report, see Standard Document, Internal Investigations: Investigation Report.
- **Ensure the completion of correction actions.** The company should develop protocols for:
  - verifying that corrective actions have been completed; and
  - escalating cases when remediation falls behind schedule.

Eight: Due Diligence and Oversight of Third-Party Relationships

The actions of third parties can create significant compliance risk for a company. To manage this risk, the company should implement compliance requirements to oversee its third-party relationships, including:

- Conducting risk-based due diligence of third parties.

- Obtaining commitments to compliance from its transaction counterparties.
- Warning and even terminating relationships with third parties who fail to behave in a compliant manner.

Risk-based due diligence is the process by which the company determines the level of due diligence to conduct based on the level of risk posed by the third party. For example, key issues to consider in assessing the level of corruption risk posed by third parties include industry and location. High-risk industries include areas that are highly regulated or require government approvals (such as construction, defense, and mining). High-risk countries include those with a high perceived level of public sector corruption. The Corruption Perceptions Index (CPI), developed by Transparency International, ranks approximately 180 countries on a scale of "highly corrupt" to "very clean."

The DOJ and SEC consider risk-based due diligence in assessing the effectiveness of a company's compliance program (see FCPA: A Resource Guide to the U.S. Foreign Corrupt Practices Act). The company should conduct risk-based due diligence on its:

- Target companies in a **merger** or acquisition (see Practice Note, M&A Due Diligence: Assessing Compliance and Corruption Risk).
- Joint venture, investment, and other business partners (see Practice Note, Due Diligence Considerations in Joint Ventures).
- Agents, consultants, and other third-party representatives (see, for example, Foreign Corrupt Practices Act Compliance Checklist: Develop a Risk-based Assessment for Each Jurisdiction and Review All Intermediaries). For a sample policy to govern the engagement of third parties and agents, see Standard Document, Policy for the Use of Third-Party Agents Outside of the United States.

For information on screening parties against applicable government watch lists, see Build a Team of Compliance Personnel.

For more information on risk-based due diligence, see Practice Note, Risk-Based Due Diligence of Third Parties in Commercial Transactions and Developing a Risk-Based Due Diligence Program Checklist.

Nine: Monitoring and Auditing of Program Effectiveness

To ensure that the compliance program is effective and being followed, the company should:

- **Continuously monitor the program.** The CCO should:
  - continuously monitor the company's ongoing operations to verify that internal controls, policies, and procedures are in place and being followed;
  - conduct regular self-assessments of the compliance function using analyses of compliance trends within the company, such as hotline statistics, feedback on compliance matters, and reviews of high-risk areas;
  - identify compliance gaps where standards have not been fully understood or implemented and other program or operational weaknesses that may require more detailed evaluation or auditing. For example, the company should review if employee training requirements are being met, employee and vendor screenings are being conducted, or disciplinary action is occurring and is appropriate; and
  - determine opportunities for program improvement.
- **Proactively audit the program.** The CCO should coordinate with auditors independent from the compliance function, such as the company's internal audit staff or external auditors, to:
  - check that the compliance program's monitoring function is operating as it should;
  - systematically test the program using employee interviews and surveys, on-site visits, and spot checks to evaluate if the internal policies, procedures, and controls adopted by the company are adequate, up-to-date, understood, and effective in reducing risks;
  - regularly conduct targeted, in-depth audits of high-risk areas for the company to check compliance with company policies and applicable laws and regulations. For example, for guidance on conducting wage and hour, health and safety, **trademark**, **Section 409A**, and antitrust audits, see Practice Notes, Conducting an Internal Wage and Hour Audit, Minimizing OSHA Liability Through Voluntary Safety and Health Audits and Trademark Audits, Section 409A Preliminary Internal Audit Checklist and Antitrust Audit Checklist;
  - understand if employees are comfortable reporting non-compliance and how they view the company's commitment to compliance;
  - measure the compliance program's effectiveness and benchmark findings against previous year results; and
  - make recommendations for program improvements.

- **Report the monitoring and audit results.** The CCO should keep the governing body and senior management informed of the program's monitoring and audit results, determinations of program effectiveness, and recommendations for program improvements.
- **Update the program as necessary.** Program updates should take into account the results and recommendations developed from the company's monitoring and audit activities.

Ten: Ongoing Risk Assessment to Maintain Program Effectiveness

Re-assessing the company's legal risks on an ongoing basis is required to maintain an effective compliance program in an ever-changing risk landscape. The company should:

- Analyze its enterprise-wide business activities (taking into account any new business or geographic areas for the company) at least once a year to update its risk profile.
- Identify opportunities for continuous improvement by evaluating factors such as:
  - program audit results, including employee feedback;
  - compliance reports;
  - changes to applicable law, including at the local level;
  - recent litigation and claims;
  - results of benchmarking against the practices of comparable companies;
  - evolving industry standards and new industry enforcement trends; and
  - new regulatory guidance on compliance programming. For example, the DOJ published general guidance in February 2017 (Evaluation of Corporate Compliance Programs) and specific antitrust guidance in July 2019 (Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations) to help companies design and implement corporate compliance policies and procedures. The guidance documents explain how the DOJ evaluates compliance programs in its criminal investigations.
- Modify and tailor each compliance program element to address the updated risk profile and the specific needs of the organization. This should include setting up a process to re-allocate compliance resources to the highest priority risks.
- Coordinate the compliance risk assessment with the company's enterprise risk management (ERM) program. For information on enterprise risk management, see Article, Enterprise Risk Management.

Additional Steps to Enhance a Compliance Program

Integrate Mergers and Acquisitions

Post-acquisition integration is vital to developing an effective compliance program that permeates an organization. To ensure that a newly merged or acquired company (the acquired target) promptly comes into compliance with applicable laws, the company should:

- Conduct a post-acquisition risk assessment and audit of the acquired target, including a review of the acquired target's:
  - compliance program and the personnel responsible for its oversight (see Conduct an Initial Risk Assessment and Three: Oversight, Autonomy, and Resources for the Compliance Function);
  - high-risk geographic areas and high sales volume areas where the acquired target does business to determine the compliance risks prevalent in those areas (see Conduct an Initial Risk Assessment); and
  - contracts with agents, consultants, and other third-party representatives. Particular attention should be paid to the engagement's geographic scope, type of activities, level of oversight, and amount of commission paid, as well as any pre-acquisition due diligence reports (see Eight: Due Diligence and Oversight of Third-Party Relationships).
- Promptly incorporate the acquired target into the company's internal controls, including the company's code of conduct and overall compliance program.

- Train directors, officers, and employees of the acquired target, and where appropriate, train its agents and business partners, on the company's compliance policies and procedures (see Four: Ongoing Training and Communication on Compliance Matters).
- Disclose to the relevant government agency, if appropriate, any non-compliance discovered during the due diligence process.
- Expand the compliance program to meet the company's growth needs. An effective program grows with the company after iterative risk reassessment.

For more information on integration following the closing of a merger or acquisition, see Practice Note, Preparing the Buyer for Post-Closing Integration and M&A Integration Checklist.

Document Compliance Efforts

The company should thoroughly document compliance measures and retain supporting materials so that in case of a compliance failure it has a clear and orderly record to:

- Assure stakeholders (such as investors and business partners) of its commitment to a corporate culture of ethics and compliance.
- Demonstrate to regulators the actions it took to prevent and detect the misconduct.
- Explain to regulators why those compliance measures were reasonable.
- Receive cooperation credit from regulators for having an effective compliance program.

To document its implementation of the core program elements identified in the Sentencing Guidelines (see Ten Hallmarks of an Effective Compliance Program), the company can use a tracking tool such as SharePoint (if available), an Excel spreadsheet, or other tracking method. In particular, the company should be sure to track and document:

- **Compliance activities of the governing body.** Documenting the governing body's efforts to oversee the compliance program, including its receipt and review of periodic reports and updates and its program approvals and compliance-related resolutions, helps demonstrate a strong, ethical tone from the top (see One: Strong Organizational Leadership and Ethical Culture).
- **Training sessions and follow-up communications.** As the company trains its directors, officers, employees and, if appropriate, agents and business partners on relevant compliance issues, it should maintain records of:
  - training dates;
  - materials used;
  - attendance;
  - completion of training; and
  - compliance certifications signed by training participants.
- **Due diligence activities.** The DOJ and other regulators consider the appropriateness of a company's due diligence activities in determining the adequacy of a company's compliance program. The company should document its due diligence of:
  - compliance personnel;
  - joint venture and other business partners;
  - acquisition targets; and
  - agents, consultants, and other third-party representatives.
- **Compliance-related reports and the responses to those reports.** The company should:
  - track the number and type of compliance-related reports it receives;
  - document its determination of the follow-up required; and
  - record its responses to the reports.

This documentation creates a record for the company in case of a government audit or investigation. It also provides a basis for the company to create reporting statistics and analyze trends in its compliance program.

- **Internal investigations.** Documentation of an internal investigation should include:
  - tracking of progress, duration, and status to ensure that reports are fully and timely investigated and addressed as needed;
  - a description of the issues investigated;
  - a summary of persons interviewed (including the source of the allegations, if available) and evidence considered;
  - a summary of findings; and
  - the outcome of the investigation.

  For more information on:
  - documenting an internal investigation, see Standard Documents, Internal Investigations: Investigation Report and Internal Investigations: Witness Interview Memorandum;
  - creating and maintaining the attorney-client privilege and **work product protection** over documents created during an investigation, see Practice Note, Internal Investigations: US Privilege and Work Product Protection; and
  - preserving documents in anticipation of government investigation, see Practice Note, Implementing a Litigation Hold and Litigation Hold Toolkit.
- **Remedial actions.** Both the DOJ and the SEC emphasize the importance of initiating remediation steps as soon as possible during an investigation and regularly credit companies for those efforts. Documenting all remedial actions implemented by the company to mitigate harm caused by a violation is important for the company to receive credit and mitigate liability.
- **Disciplinary measures.** Among the factors prosecutors consider are whether the company appropriately disciplined wrongdoers, regardless of the status or position of the individuals. Documentation of fair and appropriate discipline of employees and managers who have engaged in misconduct can help demonstrate the company's commitment to compliance and ethics both in what it says and does.
- **Compliance program reviews and continuous improvement actions.** Companies change over time through natural growth, mergers, acquisitions, and other business transitions. The company should document any adjustments and improvements made to the compliance program based on changes in the law, business practices, and other risk assessment and monitoring and audit results. This record of program changes can help the company demonstrate that the program has evolved and grown and continues to be effective.

The company should maintain its documentation of compliance efforts in accordance with its record retention policy. For general guidance on retaining and disposing of company records, see Practice Note, Drafting a Document Retention Policy and Records Management Toolkit.