Compliance 360°

White Paper:
The Seven Elements of an Effective Compliance and Ethics Program

Executive Summary

Recently, the United States Sentencing Commission voted to modify the Federal Sentencing Guidelines, including the standards for an effective corporate compliance and ethics program. These guidelines have become an important barometer used by federal prosecutors and regulators in determining whether a company should be charged with a crime at the conclusion of an investigation, and if so, the severity of the civil enforcement action. Forward thinking organizations seeking to develop and foster an effective compliance and ethics program are turning to Governance, Risk Management and Compliance (GRC) software applications to help facilitate this endeavor. This document describes the seven elements of an effective compliance and ethics program and the key capabilities that a GRC software solution should have in order to serve as the foundation for an effective compliance and ethics program.

1185 Sanctuary Parkway, Suite 250, Alpharetta, Georgia 30004 I Phone: 678.992.0262 I www.compliance360.com

Introduction

The United States Sentencing Commission voted on April 7, 2010 to modify the Federal Sentencing Guidelines for organizations, including the provisions that set forth the attributes of effective compliance and ethics programs. Under the Federal Sentencing Guidelines, which go into effect on November 1, 2010, a convicted organization may be eligible for a reduced sentence if it has established an effective compliance and ethics program. The Guidelines describe the key attributes that a compliance and ethics program must exhibit for the organization to be eligible to receive benefits such as reduced fines, reduced sentence or deferred prosecution.

Beyond the potential benefits related to prosecution and conviction, the key attributes within the Guidelines have become widely used by organizations seeking to proactively establish effective compliance and ethics programs. Satisfying the requirements for an effective compliance and ethics program is now widely believed to create a number of additional benefits including protection of the corporate brand by reducing the likelihood of bad events and minimizing the consequences should bad events occur.

The seven elements are summarized as follows:

1. Establish Policies, Procedures and Controls
2. Exercise Effective Compliance and Ethics Oversight
3. Exercise Due Diligence to Avoid Delegation of Authority to Unethical Individuals
4. Communicate and Educate Employees on Compliance and Ethics Programs
5. Monitor and Audit Compliance and Ethics Programs for Effectiveness
6. Ensure Consistent Enforcement and Discipline of Violations
7. Respond Appropriately to Incidents and Take Steps to Prevent Future Incidents

(1) Establish Policies, Procedures and Controls

Organizations must establish standards, procedures and controls to prevent and detect unethical conduct. According to the Guidelines, these standards of conduct and internal controls should be reasonably capable of reducing the likelihood of misconduct. The standards should be incorporated into a written code of conduct that enables audit systems and other procedures to have a reasonable chance of preventing and detecting wrongdoing.

An effective GRC software solution must enable an organization to create, organize, and manage the life cycle of policies and procedures. Policy and procedure documents are managed electronically from start to finish, including collaboration, approval, revisions, and revision history. Users should have the ability to search through approved policies to read them with access limited to appropriate parties via security controls.

Key capabilities should include:

- Ability to establish a central repository for full life cycle management of policies and procedures including authoring, approvals, version control, audit trail, archive and alerts.
- Ability to manage policies using a centralized corporate model or distributed autonomous model or hybrid approach. The system should also provide support for sharing best practices among divisions.
- Automate policy authoring and revisions, reviews, approvals and distribution with built in workflow.
- Automate reminders for key policy dates such as reviews, revisions and expirations.
- Link policies and procedures to laws and regulations. This is critical for efficiently demonstrating proof of compliance during an audit or exam.
- Provide an easy, secure policy search for all constituents, including individuals in that may not necessarily have user rights to the software.
- Ability to monitor policies and policy management activities with a variety of configurable reports and online dashboards.

(2) Exercise Effective Compliance and Ethics Oversight

Organizations must involve multiple layers of management in the compliance and ethics process with the goal of ensuring the effectiveness of the programs. Designated individuals in each management level must be appropriately knowledgeable of the program. The Guidelines impose specific duties on various levels of management including the board of directors, senior management and individuals with primary responsibility for the compliance and ethics programs.

An effective GRC software solution must enable an organization to configure and organize their relevant information in a consolidated "role-based" view, providing facilities such as personal home page dashboards. The solution should also be equipped with alerts and reminders to support the appropriate level of awareness and timely actions that may be needed.

Key capabilities should include:

- Task lists, calendars and reminders that serve as a "compliance inbox". The status of any tasks that have been assigned by other users, or automatically by the system should be listed here. Users can also receive task notices in their e-mail inbox.
- Charts and graphs that are automatically updated based on selected criteria. Charts and graphs should also provide direct drill-down to underlying details to support rapid analysis of root cause issues.
- Links to preconfigured reports that provide up-to-date information based on criteria that the individual has specified.
- Automated links to news feeds for articles and publications relevant to compliance, risk management and audit management topics. These should also be capable of providing access to the latest updates from the regulating agencies.

(3) Exercise Due Diligence to Avoid Delegation of Authority to Unethical Individuals

Organizations must use reasonable efforts to avoid delegating substantial authority to individuals with a history of engaging in illegal activities or other behavior inconsistent with an effective compliance and ethics program.

Many organizations today are increasingly more reliant on third parties to handle a variety of outsourced operational functions. Outsourcing functions that are beyond an organization's core strengths makes good business sense, however, organizations must also use proper safeguards to ensure they are dealing with reputable and ethical organizations as you cannot outsource your liability along with operational functions.

An effective GRC software solution should include surveying capabilities allowing an organization to create and manage data collection surveys, analyze the results, and initiate remediation plans if necessary. The distribution of policies, such as the code of conduct, should support the use of surveys to collect and confirm attestations such as those related to conflicts of interest. Incorrect and inappropriate answers to survey questions should be used to indicate a lack of understanding, regardless of the accompanying attestation, and in turn, used to assign remediation tasks.

In addition to managing and confirming employee attestations, an effective GRC software solution should also include Third Party Risk Management capabilities enabling an organization to address the critical requirements of vendor compliance and risk management. The application should provide high-level risk profile charts to monitor risk trends, identify "watch list" organizations and proactively identify underlying causes of increasing risk.

Key capabilities should include:

- Distribute documents such as policies and procedures, along with verification-of-understanding questions to all personnel, third parties, or vendors.
- Automate data collection and the distribution of results using an automated facility such as workflow.
- Automate the processes of confirming attestations, identifying gaps and initiating remediation tasks.
- Link survey results and follow-up actions to their related laws and regulations. This is critical for efficiently demonstrating proof of compliance during an audit or exam.
- Monitor surveys, results and follow-ups with configurable reports and online dashboards.

(4) Communicate and Educate Employees on Compliance and Ethics programs

The organization must take reasonable steps to communicate periodically and in a practical manner, its standards and procedures, and other aspects of the compliance and ethics programs throughout all levels of an organization, including senior management and the board of directors.

To address these requirements, an effective GRC software solution should act as a "compliance system of record" enabling an organization to manage and disseminate information regarding regulations change and generate automated alerts to ensure that the appropriate individuals are kept abreast of the latest updates. Then, as new policies are authored or existing policies are revised and approved, the system can be used to keep employees informed through education and training. The system should streamline internal risk assessments (centralized or distributed), as well as the development of action plans for areas identified as having compliance gaps, and the creation of a dynamic body of evidence of compliance.

Key capabilities should include:

- The system should automatically receive new and updated laws and regulations from a variety of external sources, and initiate risk assessments based on changing laws and regulations.

- Automate the distribution of new and revised policies and compliance assessments to all relevant personnel.
- Provide education and training of new or revised regulations and policies
- Automate compliance gap assessments as well as remediation plans and projects using an automated facility ion such as workflow.
- Provide a forum or message board to serve as a knowledge base of authored research and "frequently asked questions" (FAQ) relative to compliance and legal issues, as well as, facilitated communication and collaboration throughout selected levels of the organization.
- Link all evidence of compliance to each law and regulation. This is critical for efficiently demonstrating proof of compliance during an audit or exam.
- Monitor regulatory compliance status using configurable reports and online dashboards.

(5) Monitor and Audit Compliance and Ethic Programs for Effectiveness

Organizations must ensure that the compliance and ethics programs are followed by employees. They must also create mechanisms for auditing and reporting on the effectiveness of the programs.

As with the other key elements of effective compliance and ethics programs, an effective GRC software solution acting as a "compliance system of record" should enable an organization to support this requirement. Automating scheduled compliance assessments on a quarterly or even monthly basis should enable an organization to closely monitor high risk areas and assign the necessary remediation tasks and deadlines. The remediation projects should be captured in the system and the data made available via dashboards and alerts to all stakeholders. By providing this level of visibility, managers, executives and/or board members should be able to monitor relevant information and maintain an always-up-to-date awareness of the organization's compliance status. Additionally, key compliance areas identified as deficient should be targeted for internal audits.

An effective GRC software solution should support the entire audit process including the management of risk assessments, development of audit plans and associated audits, definition of audit objectives and steps, tracking audit activities, generation of work papers, development of findings and recommendations, and the management of remediation plans.

Key capabilities should include:

- Improve visibility and control by serving as an internal audit system of record.

- Comprehensive audit plan management throughout the life-cycle of each audit, including resource assignments and work-plan creation.
- Manage and track tasks and staff time.
- Complete meeting management with tracking of meeting agendas, attendance and minutes.
- Graphical reporting of audit activities, statuses, and results.
- Document recommendations, management responses and oversight of remediation projects.
- Monitor internal audit activities with a variety of robust, configurable reports and online dashboards.

(6) Ensure Consistent Promotion of the Program and Enforcement of Violations

The Guidelines indicate that organizations should consistently promote the value and importance of compliance and ethics programs. Organizations should reward those actions that demonstrate adherence to an ethical culture and discipline individuals who fail to adhere to the organization's ethical standards.

To further enable the corporate integration of compliance programs with a GRC software solution, the system should provide the ability to securely access widely used corporate functions, such as policy searches, directly from the corporate intranet. Additionally, the system should possess the ability to take on the look and feel of other, already familiar corporate applications and adopt the organization's standards and branding.

Regarding the enforcement requirements for consistent rewards for ethical behavior and discipline of ethics violations, an effective GRC software solution should be used, just as it is used to manage policies tied to other regulatory requirements. Rewards and disciplinary policies should be drafted and then circulated (using workflow automation), for review, edit and final approval. Once the enforcement policies are finalized, workflow should automatically distribute the policies to all relevant parties. The compliance assessment capabilities previously described should be used to identify compliance gaps and assign remediation tasks and deadlines.

Additionally, an effective GRC software solution should have the ability to capture and store a variety of reportable events or "incidents" to help ensure enforcement after an incident occurs. Enforcement actions and other follow-up tasks related to each incident should be assigned and centrally monitored to ensure proper follow through.

As previously mentioned in the other elements, surveying functionality should support dissemination of questionnaires related to key elements of the compliance program. For example once a year, each employee may be scheduled to receive a survey that promotes

that organization's compliance program. The survey would likely request an attestation regarding the reading and understanding of the materials along with questions used to confirm the attestation.

Key capabilities should include:

- Ability to establish a central repository for full life cycle management of policies and procedures including authoring, approvals, version control, audit trail, archive and alerts.
- Distribute new and revised policies and compliance assessments to all relevant personnel
- Ability to collect, store, and collaborate on compliance-related incident information and track the progress of investigations.
- Confirm attestations, identify gaps and initiate remediation tasks.
- Link survey results and follow-up actions to their related laws and regulations.
- Monitor surveys, results and follow-ups with configurable reports and online dashboards.

(7) Respond Appropriately to Incidents and Take Steps to Prevent Future Incidents

The Guidelines require that organizations take appropriate investigative actions in response to suspected compliance and ethics violations. Organizations should also take appropriate steps to preserve the confidentiality of investigations.

As mentioned in the previous element, an effective GRC software solution should possess the capability to capture and store incident information. This functionality enables organizations to manage a wide variety of issues such as hotline tips, potential fraud and abuse occurrences, audit findings, legal cases and even everyday occurrences such as workplace accidents. In keeping with the concept of a "compliance system of record", the system should provide a repository of incident information, allowing departmental personnel to collaborate and track the progress of investigations while automating maintenance of compliance logs and overall compliance management. Corrective actions and other follow-up tasks related to each incident should be assigned and centrally tracked as needed to prevent future incidents and compile a body of proof of preventative measures. Additionally, all incident information should be included in reports and graphically represented in online dashboards to demonstrate trends and correlations.

Using the "compliance system of record", incidents, investigations and corrective action plans should be linked back to applicable laws and regulations, to create a dynamic body of evidence of compliance and ensure a continual audit-ready state for the organization.

Key capabilities include:

- Create a central repository for managing and tracking incident information and follow-up actions and outcomes. Consolidate incident / case tracking databases.
- Automate investigation processes, task assignments and reminders using the workflow engine.
- Link incidents to laws and regulations. This is critical for efficiently demonstrating proof of compliance during an audit or exam.
- Integrate external hotlines into the incident management process to provide additional automation and preserve anonymity.
- Securely transfer sensitive incident information between departments.
- Assign individual tasks and track the status of follow-up and corrective actions.
- Monitor incidents and trends with configurable reports and online dashboards.

Conclusion

As a result of the United States Sentencing Commission's recent modifications to the Federal Sentencing guidelines, organizations should establish compliance and ethics programs rooted in these guidelines and evaluate existing corporate compliance and ethics programs to ensure that they conform. By establishing effective compliance and ethics programs and satisfying the requirements in the Guidelines, organizations are eligible to receive benefits such as reduced fines, reduced sentence or deferred prosecution. Aside from the benefits of reducing the severity of civil enforcement action, establishing an effective compliance and ethics program just makes good business sense and can enable organizations to better protect the corporate brand by reducing the likelihood of bad events and minimizing the consequences should bad events occur. Organizations looking to establish an effective compliance and ethics program should consider adopting Governance, Risk Management and Compliance (GRC) software applications to serve as the foundation of their program and consider the key capabilities highlighted in this document when selecting a solution.

About Compliance 360

Compliance 360 is a comprehensive solution that serves as the "compliance system of record" as it streamlines governance, risk management and compliance (GRC) process across the enterprise. The system is designed to make compliance, audit and risk management easier, less costly, and much more manageable – especially for organizations in highly regulated industries. With Compliance 360, you have a highly configurable set of applications that help you identify compliance gaps, eliminate duplicate efforts and easily maintain the records needed to demonstrate full compliance. To learn more about Compliance 360 and specific capabilities for establishing effective compliance and ethics programs, please contact us at www.compliance360.com/contact.asp.