



CIS WHITE PAPER
2009

Building a Compliance Program



*Chris Cobourn, CIS, VP, Regulatory
Compliance*



*Clarissa Crain, CIS, Senior Compliance
Specialist and Audit Lead*

“Drug companies that do not have a compliance strategy in place may soon pay a very high price.”

Deborah Autor, Director of Compliance at FDA's Center for Drug Evaluation and Research (CDER)

The concept of Commercial Compliance in U.S. manufacturing has evolved very quickly over the past five or six years, resulting in increased regulatory requirements and investigation activity. While the security of the supply chain and the ethical promotion of drugs has been a significant focus, recent investigative trends show a shift in the Government's focus. The U.S. Federal Government and various State Governments are becoming increasingly interested in sales, marketing and distribution activities that ultimately affect the sales or prices witnessed by the Government.

The need for a manufacturer to understand and mitigate the risk of doing business with U.S. Federal Government is real. Various enforcement agencies exist across State and Federal Government. The Office of the Inspector General (OIG) which supports the Health and Human Services (HHS) is one of the most common enforcement agencies representing the Federal Government in the Commercial Compliance space. Responsible for the prevention and detection of fraud, waste, abuse and mismanagement in programs legislated by the Social Securities Act, the OIG conducts and supervises audits, evaluations and investigations within Commercial Compliance.¹

Key Agency Initiatives:

- Swift, aggressive enforcement of action
- Civil monetary penalties
- Increased scrutiny of data integrity, global operations and unapproved drugs

The best, most appropriate measure of the effectiveness of a manufacturer's risk management program is to evaluate it against a standard of enforcement agency audit. Utilizing OIG Audit Readiness as a standard of measure helps develop the highest level of compliance.

With senior management aligned on risk, and by establishing your audit and monitoring programs to manage risk, you can develop transparency and a roadmap that will demonstrate that you take compliance seriously and have developed an effective Compliance Program. So don't make monitoring and audit the "tail of the dog" that you apply at the end; use it up front to define your strategy and develop better compliance.

¹ Mission. <http://www.oig.hhs.gov/>. Accessed February 15, 2009.

I. Developing a Risk Profile and Risk Management Program

Through a series of steps, you can develop a Risk Profile and a Risk Management Program, with monitoring and audit as key components.

Step one is to understand the Government's view of risk. A manufacturer can get a clear understanding of the OIGs view of risk by reviewing the following:

- The OIG Recommendations to Pharmaceutical Manufacturers, April 2003.ⁱⁱ This document creates an outline of "Commercial Compliance," by defining the Government's view of the three key risk areas, and provides an outline for a Corporate Compliance Program.
- The OIG Work Plan. The annual Work Plan outlines areas where the OIG intends to put its audit focus, and includes sections specifically for manufacturers. (Remember, the OIG is now budgeted for proactive audits!)
- Recent Investigations and CIA's. These show the trends in investigative activity, how the Government interprets statutes, such as the False Claims Act and FDA guidelines on Off Label promotion, as well as the evolving and complex nature of CIA's (including audit and monitoring provisions).
- The new PhRMA code. Although this is not an OIG or Government document, it does show the industry's focus on developing guidelines to manage key risk areas, such as interactions with healthcare professionals.
- Applicable Regulations and Guidance - it is also important, to follow the actual guidance in the Commercial areas.

Step two is to conduct an initial assessment. The initial assessment activity must be deep enough and broad enough to look at all of the potential risk areas. The initial assessment can be used as the basis for developing your Risk Profile and your Risk Management Plan, and will identify compliance gaps so that you can develop a management action plan.

ⁱⁱOIG Compliance Program Guidance for Pharmaceutical Manufacturers. Federal Register. Volume 68. Number 86. April 23, 2003.

Step three, develop the plan and roadmap. As a result of the assessment activity, you will be able to identify compliance risks which may require immediate attention, develop a Risk Profile based upon the findings (matching the defined Government risk areas to your company), and develop a Risk Management Plan and a roadmap.

Step four is alignment. This is often the hardest step, as it can involve a change in the corporate

culture. This involves bringing the results of the assessment to senior management and the Compliance Committee. This can be done in a coordinated effort between Internal Audit, the Compliance Officer, and Internal Counsel. Alignment on the Risk Profile and Risk Management Plan is necessary for the Compliance Officer and Internal Audit to develop a plan that is achievable, and has management agreement.

With an evaluation of risk complete and prioritized, a company must now develop a Risk Management Strategy. Commercial Risk Management is a strategic program designed to decrease compliance risks by using one or more evaluation techniques to identify potential risk. Evaluation techniques may vary, however the most effective Risk Management programs use two or more techniques/tools to proactively identify and mitigate potential risk. The OIG defines Risk Management as seven elements of compliance, with core elements defined as: Auditing and Monitoring, Enforcing Standards through Well-Publicized Disciplinary Guidelines and Responding to Detected Offenses and Developing Corrective Action Initiatives.

OIG's Seven Elements of a Successful Compliance Programⁱⁱ

1. Implementing Written Policies and Procedures
2. Designating a Compliance Office and Compliance Committee
3. Conducting Effective Training and Education
4. Developing Effective Lines of Communication
5. Conducting Internal Auditing and Monitoring
6. Enforcing Standards through Well-Publicized Disciplinary Guidelines
7. Responding to Detected Offenses and Undertaking Corrective Action

ⁱⁱOIG Compliance Program Guidance for Pharmaceutical Manufacturers. Federal Register. Volume 68. Number 86. April 23, 2003.

II. Developing a Monitoring, Testing and Auditing Function

In order to develop an appropriate monitoring, testing, and auditing function, it is important to first understand the current or baseline status of the respective area for which a Risk Management Program is being developed. Even if a defined Risk Management Program does not exist within a company, there are often some monitoring and auditing functions present. These functions may not be clearly defined as such, and so through the Assessment phase of Risk Management development, they can be identified and formalized. From a monitoring perspective, internal controls, business metrics, management reviews, and routine self assessments all represent potential monitors. Additionally, Sarbanes Oxley (SOX) testing and internal audit functions represent auditing functions which may overlap with Compliance Audit. Reviewing existing monitoring and auditing functions and developing a Business and/or Risk Assessment based on the identified gaps will help to ensure an effective and meaningful Risk Management Program is developed.

Monitoring

Monitoring, typically defined as the first step in an effective Risk Management Program, is defined as the ongoing, real-time checks and balances implemented and executed by a functional/operational group to ensure proactive evaluation, identification and mitigation of risk. It is a company's first line of defense. Carried out on a routine, if not daily basis, monitoring is the responsibility of respective functional/operational process owners. Monitoring differs from control activities in that monitoring is a review function.

Monitoring looks at execution across an entire process, including controls, to ensure that processes are being performed appropriately and are meeting business requirements. Monitors should be built into departmental processes and reviewed, if not executed, by functional/operational

area management. Identified trends or risks could result in process improvements including changes to process flows and updates to departmental process documentation.

An effective monitoring program should meet the following criteria:

- Conducted on an ongoing basis
 - Completed or overseen by departmental management
 - Review of all key controls
 - Identified risks or process changes are mitigated/implemented
-

Testing

Testing is the Risk Management phase which is conducted periodically by a party once removed from the functional/operational area being evaluated. Similar to audit in many capacities, testing is distinguished from audit by its more frequent occurrence and more limited or specific scope. Tests are typically developed based on the identification of key risk areas. Through an assessment and prioritization of risk, a Test Plan can be developed outlining the anticipated scope and timing of given tests.

Tests, in support of the Test Plan, can be developed in many different ways. Some companies choose to identify controls and test activities executed against key controls (similar to SOX), other companies choose to test process components based on Risk Assessment. There is not a prescriptive definition for what testing is or is not; however, at a minimum it must ensure that monitors and controls are working effectively and providing the appropriate level of assurance that compliance is being maintained on an ongoing basis.

Test scripts document frequency, timing, scope, sample size and test criteria for each test defined in the Test Plan. Developing test scripts can be challenging for an individual that is removed from a given functional/operational role. In order to ensure that test scripts are appropriately developed, the developer should reference the department's guiding policies and procedural documentation. This documentation should sufficiently outline

controls, monitors and processes related to the group's responsibilities. Should it be found that policy and procedure documentation is insufficient in defining these components, departmental staff interviews may be necessary in order to obtain the necessary information.

Tests should be executed in alignment with the Test Plan and documented test scripts. Test results are documented within the test scripts and in management reports. Results should be provided to functional/operational area management and to senior company management as appropriate. Risks or potential risks identified through testing must be mitigated. It is not the responsibility of the tester to mitigate identified risks. The tester reports identified risks and potential risks to the appropriate management and it is the responsibility of management to execute corrective action/ mitigating risk plans. Testers may choose to make recommendations on how to appropriately mitigate a risk; however, it is not required.

The effectiveness of a Testing program can be evaluated by the function's ability to identify key risks and communicate those risks to management.

If a Testing program is working appropriately, it is evaluating a functional/operational group against Government regulations, company policy and departmental process documentation.

Auditing

Internal Audits are part of a standard Risk Management Program and are proactive in nature (as opposed to reactive investigations). Executed by an independent party, an audit is a holistic review and identification of risk. The frequency of an independent audit is driven by multiple factors including a company's audit resources and the risk associated with a given function or operation.

Similar to testing, an Audit Plan is developed based on assessed risk. Execution against the Audit Plan may happen through detailed scripting, or occur as a less rigid review of a given process. Findings from an audit are documented and communicated to both functional/operational management and senior management. Like testing, corrective action and/or mitigating action plans are not the responsibility of the auditing party. Instead, it is the responsibility of the respective management to ensure the appropriate action is taken to mitigate identified or potential risk.



When evaluating the effectiveness of an Audit Program, ask the following questions:

- Are Audits conducted at the appropriate level and at the appropriate frequency, relative to risk?
 - Are Audits conducted by individuals with the appropriate level of subject matter expertise?
 - Are the Auditors independent of influence or bias related to a given function or process?
 - Are Auditors evaluating processes from a compliance perspective, and not financial or other?
-

An effective Audit Program will identify any potential gaps or risks not identified through monitoring and testing. Completely independent of influence or bias, the auditing party is able to provide an outsider's perspective on a given function or compliance process. When executed proactively, the auditing function can help to determine a company's or department's level of "Audit Readiness."

Audit Readiness is the idea that a company should be able to efficiently, effectively and completely respond to an external audit request, thus resulting in a favorable audit outcome. Further, a proactive audit helps to show a company's commitment to ongoing compliance. As a company's final safety net, the effectiveness of an auditing function is critical.

III. Developing Action Plans and Ongoing Maintenance

Corrective and Mitigating Action Plans are arguably the most important component of Risk Management. Without appropriate response to identified risks, a Risk Management Program fails. The development and implementation of corrective actions is not the responsibility of testing or auditing parties, and therefore falls to functional/operational areas and management to ensure that the appropriate corrective actions are identified and implemented. Having a party responsible for the oversight of the corrective action plan is highly recommended. Most companies choose to utilize a compliance department or senior manager in this function.

The individual or department tasked with oversight of corrective actions is not responsible for implementing the actions, but instead assuring that functional/operational staff implements the actions and that they are appropriate based on the identified or potential risk. Based on these implemented corrective and mitigating actions, it is likely that a given functional/operational area's processes will need to be updated, thus leading to subsequent updates and changes to existing controls, monitors, tests and audit plans.

Risk Management Maintenance

The goal of Risk Management is to be both preventative and detective in identifying existing and potential risk. In order for a Risk Management Program to be effective, the program must be routinely evaluated and updated. Changes in business processes, updates to processes and controls based on corrective actions, revisions to company policies or departmental process, and changes in legislative guidelines can all drive updates to a Risk Management Program.

A Risk Management Program that is not routinely reviewed and updated is not effective. It is recommended that companies identify an owner for the Risk Management Program. The owner is responsible for coordinating updates, staying abreast of business and regulatory changes, and conducting ongoing assessments of business risks. Without this commitment, even the best built Risk Management Program will eventually fail to provide the level of scrutiny needed to protect the company and ensure ongoing compliance.

IV. How CIS Can Help

Compliance Implementation Services (CIS) is a consulting firm specializing in compliance strategies for pharmaceutical companies, from Global Clinical Research & Development through U.S. Commercial Compliance and Government Programs. Founded in 2004, our deep understanding of industry laws and regulations, innovative and practical applications and custom solutions help our clients establish a “Culture of Compliance” that is both meaningful and practical.

Our experts quickly identify your exposure to compliance risks, help you develop a strategic plan and ensure its implementation and ongoing adherence to legal and regulatory requirements.

Our Areas of Expertise

- Policy & SOP Development, Review and Harmonization
- Risk Management Processes, Audits and Assessments
- System Evaluation, Implementation and Validation
- Training Development and Delivery
- Strategic Outsourcing

Culture of Compliance Lifecycle

CIS can help define and develop the key components of a solid Compliance Program, starting with understanding risk specific to your organization, and developing a strategy that enables you to manage risk effectively within your business. We offer extensive industry experience and expertise in this area to help implement and maintain your Compliance Program.



CIS

484.445.7200
Media, PA

919.463.1990
Morrisville, NC

Building a Culture of Compliance



www.cis-partners.com