SCCE™
corporatecompliance.org

Compliance & Ethics PROFESSIONAL®

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

OCTOBER 2018

Meet Eric Feldman

CCEP-I, CFE

Senior Vice President
Affiliated Monitors, Inc.
Los Angeles

Contents

October 2018

FEATURES

DEPARTMENTS

COLUMNS

Compliance & Ethics Professional is printed with 100% soy-based, water-soluable inks on recycled paper, which includes 10% post-consumer waste. The remaining fiber comes from responsibly managed forests. The energy used to produce the paper is generated with Green-e® certified renewable energy. Certifications for the paper include Forest Stewardship Council (FSC), Sustainable Forestry Initiative (SFI), and Programme for the Endorsement of Forest Certification (PEFC).

by Michael Yachnik, CPA, CFF

Five steps to manage data integrity risks

» In order for businesses to fully reap the benefits and opportunities of big data, they must constantly validate, secure, and maintain the company's data.

» Regulators are taking a closer look at data manipulation, across nearly every industry and around the globe.

» Company management needs to actively demonstrate its commitment to a culture of data integrity—the tone starts at the top.

» In particular, companies that produce products subject to safety standards should consider five critical steps to ensure data integrity procedures are implemented and maintained.

» Ensuring integrity throughout a company's data life cycle is imperative to mitigating risk, deterring fraud, and protecting business reputation.

Michael Yachnik *(myachnik@stoneturn.com) is a Partner at StoneTurn in New York, NY.*

In today's world, big data continues to transform the way companies do business by identifying new markets, manufacturing more efficiently, targeting consumers with personalized ads, or developing new products through more effective research and development. Despite these benefits and opportunities, the reliance on data has brought about a surge of data consumption, creating the need to constantly validate, secure, and maintain the data being used and stored.

Yachnik

This proliferation of data can be seen on a global scale, affecting every industry that manufactures products and is held responsible for testing and complying with product safety standards, including food service, children's apparel, cosmetics, farming, pharmaceutical, automotive, construction, and real estate organizations. There have been a number of high-profile data manipulation cases recently in which a company has been caught falsifying data in order to deceive its customers or product safety regulators to get a product to market. This, oftentimes, results in a costly criminal investigation and irreparable damage to the company's brand. These improprieties have raised concerns about the issue of data integrity, and to the extent to which data is complete, consistent, and accurate, they shine a light on the need to better manage, mine, analyze, and protect the data being collected, especially in assessing product safety.

With more and more instances of data manipulation being uncovered, companies and their counsel need to examine internal controls, policies, procedures, and IT systems, not only to avoid the manipulation in the first place, but also to effectively remediate issues to impede recurrence. Implementing a comprehensive data integrity compliance program is a critical step to ensure a company's processes, systems, control environment, and culture can prevent and deter data manipulation or deletion.

Here, we present five steps companies—particularly those that produce

products subject to safety regulations or standards—can take to successfully meet, or even exceed, the requirements and expectations of regulators, customers, and the public to ensure data integrity is maintained.

Develop process maps for all critical data

The importance of data collection within companies that focus on manufacturing consumer products cannot be overstated. Data is the backbone of product quality and product/patient safety decisions in these organizations. Therefore, the first step is to create an effective data integrity compliance program to identify all the critical data generated across the company, which will largely be dependent on the industry, the use of the data, and any regulatory or third-party requirements.

Once critical data is identified, its life cycle should be documented with a process map: a graphical representation of individual steps, events, operations, and systems that compose a process.

The key elements of a data life cycle are:

- **Create/acquire:** Obtain data that either did not exist or did not exist previously within the organization.
- **Process:** Transform data so it can be analyzed.
- **Analyze**: Review data with an eye toward describing facts, detecting patterns, developing explanations, and testing hypotheses.
- **Preserve**: Set procedures for saving data in a way that prevents intentional or unintentional changes or deletion.
- **Access:** Provide user-restricted access to data to aid in preparing and/or sharing it with employees, customers, and regulators.
- **Storage/reuse:** Archive data by using defined retention periods and provide ability to share data for future use.

For each of these elements, an organization needs to define the objectives and the processes in place to achieve those objectives. For example, in "Analyze," the company may be trying to determine if the results from sample testing meet the requirements of a customer. The resulting process map should describe the specific activities that occur, the data handling systems used (i.e., paper, electronic, or a hybrid of both), employees involved, equipment/instruments used, and any quality control points. Another key component that should be mapped throughout the data life cycle is the traceability system, which is a system of recorded identifications to identify information about a product throughout its life cycle. For instance, in manufacturing, a traceability system would identify all the component part sources, production line data, and line operator information for an individual finished product.

Perform a risk assessment

With data process maps in place, step two is to perform a risk assessment in order to identify, analyze, and evaluate risk in data integrity-related activities. This step is a dynamic and iterative process that requires management to consider possible changes in the external environment (e.g., regulatory changes) and adjustments to the company's own business model and processes (e.g., automation of a previously manual task). Through the risk assessment process, the organization needs to understand the controls that are in place (e.g., policy, procedure, device, practice) to minimize the occurrence or consequence of each risk.

Review policies and procedures

Next, it is imperative that all policies and procedures relevant to the data life cycle be reviewed and updated to ensure they clearly provide the necessary controls to address data integrity issues. The review process should take into account any changes in applicable

regulations, industry practices, and customer requirements, as well as adjustments within the organization, including IT policies (e.g., user rights admin, security tools, user access records, audit trails, records management), system administration, data management and storage, data acquisition and processing, data review and approval, data archiving and backup, and antifraud monitoring. For a data integrity compliance program to be effective, a procedure must be in place to communicate and provide training to all employees on changes made to existing policies and procedures.

Promote an integrity culture throughout the organization

Top-down management is a necessary step in making an effective data integrity compliance program. An organization's leadership needs to provide strong, explicit, and visible commitment to a culture of data integrity. This "tone at the top" needs to be supported through effective training, incentives aligned to company objectives, adequate resources, and appropriate procedures. Additionally, a code of conduct and ethics policies should be established, which could be further supported by a data integrity policy that sets forth: prohibition against data falsification and manipulation; direct reference to governing internal and external rules; requirements for a certification statement confirming understanding and adherence to the data integrity policy; a manner in which employees can report potential wrongful acts; and a description of how the company will investigate such reports, disciplinary actions against employees in violation of the policy, third-party requirements around data integrity, and training.

Monitor compliance

Evaluating and improving the effectiveness of a data integrity compliance program hinges on effective monitoring, which can be done through ongoing evaluations, separate evaluations, or a combination of the two. Ongoing evaluations are routine operations that are built in to business processes and performed on a real-time basis. Separate evaluations are conducted periodically by an objective party—typically an internal audit function—using a risk-based approach. Ultimately, monitoring should examine audit trails (i.e., a secure, computer-generated, time-stamped electronic record that allows for reconstruction of events relating to creation, modification, or deletion of an electronic record), and verify segregation of duties and validation of systems for intended use. Finally, when a third party is hired for activities affecting data integrity, the organization should have robust systems in place to verify and compare data generated by the contractor and should consider embedding a "right to audit" clause in the contract.

Conclusion

As companies continue their reliance on data collection and storage to increase consumer product development efficiencies, managing, mining, analyzing, and protecting data will remain a complex, costly, and concerning issue on a global scale now and into the future. Becoming an even greater challenge—particularly in the context of fraud, misconduct, and monitorships—is ensuring the integrity of the data itself. Handling these challenges requires companies to strengthen data management to verify data through its full life cycle, scrutinize how it is used to make decisions, and secure and maintain data to the highest standards. Ultimately, as regulators and customers increase their focus on quality, safety, and compliance, organizations need to be proactive in their approach to ensure data integrity. This will help companies across all industries to design and implement effective action plans to prevent and remediate the inherent risk of data integrity issues. ✳