DATA MANAGEMENT AND INDEPENDENT PRIVATE SECTOR AUDITS

A White Paper by

Douglas Hileman Consulting, LLC

Douglas Hileman, CRMA, CPEA, P.E. President

JULY 2015

A Resource for Companies Affected by

Dodd-Frank Conflict Minerals

1.0 INTRODUCTION

Section 1502 of the Dodd-Frank Wall Street Reform and Consumer Protection Act imposed a new requirement ["Dodd-Frank Conflict Minerals" or "DFCM" in this white paper] on companies that use tin, tantalum, tungsten or gold (3TG) in a product they manufacture or contract to manufacture. Some 3TG is sourced from the Democratic Republic of Congo (DRC) under conditions that benefit armed conflict, and cause or exacerbate human rights violations. National borders are porous in the region, so the DRC and adjoining countries are collectively referred to as the "Covered Countries." The Securities and Exchange Commission (SEC) promulgated a final rule on August 22, 2012 ("SEC Rule" or "the Rule"), which took effect for the 2013 [calendar] reporting year.

The SEC Rule is summarized extensively in many other publications. The basic requirements for regulated companies are listed below.

DFCM basic requirements

- Identify products that are in scope for the Rule
- Investigate the source of 3TG in the supply chain, attempting to determine the countries of origin of the minerals. This constitutes a Reasonable Country of Origin Inquiry (RCOI)
- If, upon consolidating supplier information, the regulated company has reason to believe that any 3TG in its supply chain is – or could be – sourced from a Covered Country, then proceed with additional due diligence (DD).
- Conduct due diligence in accordance with a nationally or internationally recognized standard. The OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas, Second Edition[1] ("OECD Guidelines") was identified in the Rule, and has become the de facto standard.
- Submit filings annually to the SEC, on or before May 31 following the close of the reporting [calendar] year. The filings include a Form SD (Specialized Disclosure), and, if the public issuer has conducted due diligence, the filing must also include a Conflict Minerals Report (CMR).

DFCM affects upstream suppliers in many ways; but, the IPSA applies only to public issuers subject to the Rule.

The Rule provided for two transition years – an acknowledgment that the systems and infrastructure to collect meaningful data was not available at the time. Upon completing DD, public issuers are to

[1] See http://www.oecd.org/corporate/mne/GuidanceEdition2.pdf

conclude whether their products are "DRC Conflict Free" or "Not Found to be DRC Conflict Free." During the transition years (2013 and 2014), the SEC provided an option of "DRC Conflict Undeterminable."

The Rule requires an Independent Private Sector Audit (IPSA) and specifies two objectives. An IPSA is required after the two transition years [beginning with the 2015 reporting year], unless a public issuer voluntarily elects to conclude (and report) that at least one of their products is DRC Conflict Free. Subsequent litigation and SEC guidance have deferred the requirement to state a specific conclusion about the conflict-free status of products. Pending outcome of litigation and SEC guidance, the requirement for an IPSA for the 2015 reporting year is in question as of this writing.

Regulated public issuers have submitted two CMRs. Standard practice dictates that there must be sufficient basis for any type of external communications and reporting. This is particularly true of submittals to regulatory entities with enforcement authority.

This white paper examines:

- Challenges with data management as it relates to conflict minerals programs
- IPSA background and trends
- Frameworks affecting IPSAs & data management
- Closing suggestions

Whether a company is required to procure an IPSA or not, strong data management systems and controls will provide stronger disclosures, and should help reduce risk.

2.0 CHALLENGES WITH DATA MANAGEMENT RELATED TO CONFLICT MINERALS

Business is dynamic. Developments in technology change the components of products. Fashion trends change buttons, buckles, and accessories that can contain 3TG. Companies may change their suppliers to meet market forces. Furthermore, their suppliers may change suppliers, and so forth up the supply chain.

In preparing data in support of reporting for the Rule, a company may designate cut-off dates for:

- Production of products they manufacture or contract to manufacture
- Requests for conflict minerals data of their supply chain
- Receipt of conflict minerals data from supply chain
- Further engagement with supply chain
- Receipt and acceptance of valid data from supply chain
- Preparation of SEC submittals

Many stakeholders generate requests for conflict minerals-related data.

- **SEC filings** require information on products, suppliers, RCOI, receipts of supply chain information [usually via a Conflict Minerals Reporting Template (CMRT), review of the CMRTs, and description of due diligence framework and steps taken relevant to the reporting period. The SEC filing may require an IPSA.
- **Customer requests** may include your company's CMRT, information on your DD program elements, support for data quality control, support for your company's policy, and progress on escalated issues or corrective actions.
- **Internal stakeholders** also have a variety of requests. Senior management responsible for compliance with the Rule wants to track progress towards compliance. Different groups – Procurement, Research & Development, Quality Assurance, IT, Compliance, Sales – may have responsibilities for different aspects of the conflict minerals programs. Internal Audit or Counsel may have specific requests. Requests from new customers may differ from those from existing customers.

These requests involve different information & metrics, at different points in time. This requires the ability to retrieve, sort, and report the same data in different ways. Each answer must be supportable.

Companies have taken many approaches to IT and data management for their conflict minerals programs. There are many vendors offering specialized platforms, software, or tools to manage conflict minerals data. Many companies have acquired comprehensive ERP systems with very sophisticated report writing capabilities, or built their own systems, either from common tools (i.e. Microsoft Office, SharePoint). Companies should have been thinking about the design of data management systems, and controls over data management from the outset. This will become more important as public issuers prepare for and undergo an IPSA.

3.0 IPSAS: BACKGROUND AND TRENDS

This section will discuss

- An introduction to IPSA objectives
- Frameworks and drivers
- Examples as applied to each IPSA objective
- Fraud

3.1 IPSA Objectives: Introduction

The SEC rule specifies two objectives for the IPSA. The auditor must perform procedures and express an opinion or conclusion whether:

1. the design of the issuer's due diligence framework, as set forth in the Conflict Minerals Report, with respect to the period covered by the report, is in conformity with, in all material respects, the criteria set forth in the nationally or internationally recognized due diligence framework, and
2. whether the issuer's description of the due diligence measures it performed as set forth in the Conflict Minerals Report, with respect to the period covered by the report, is consistent with the due diligence process that the issuer undertook.

Note that the IPSA does not address the completeness of the issuer's applicability of DFCM, conclusions drawn from the results of the due diligence, the sufficiency of forward-looking statements in prior SEC submittals, the feasibility of forward-looking statements in the current SEC submittal, or whether the company meets customer requirements.

The IPSA may be done by CPAs or by non-CPA auditors. IPSAs are performed to standards provided in the Generally Accepted Government Audit Standards[2] (GAGAS) – commonly referred to as "the Yellow Book." CPAs are to use attestation standards; non-CPA auditors are to use performance standards.

3.2 Frameworks & Drivers

Both of the IPSA objectives are process-oriented. Objective #1 revolves around the OECD Guidelines – which specify desired management practices and processes. Objective #2 involves support for

[2] See http://www.gao.gov/assets/590/587281.pdf

statements the public issuer includes in the CMR about the steps they took to implement their due diligence – again, a process.

The focus on processes is in keeping with decades of learning about good practices to monitor compliance and performance. Quality in manufacturing was often monitored via inspections of finished products. Even with extensive programs, quality problems persisted. Various approaches culminated in the ISO 9000 family of quality management systems standards. Similarly, ISO Environmental Management Systems were adopted in the mid-1990s to provide a more robust, ongoing approach to environmental management – and to achieve more consistent compliance.

> The requirement to have a password is a simple example of an IT-enabled control. A company may have a policy for employees to change passwords periodically. If the IT system requires users to change passwords at prescribed frequency – and prohibits users from logging in if they have not – this is a much stronger, IT-enabled control.

After the solvency issues surrounding the U.S. savings and loan industry in the 1980's, the Committee of Sponsoring Organizations (COSO[3]) developed an internal controls framework in 1992, which was subsequently updated in 2013. The U.S. Congress passed the Sarbanes-Oxley Act of 2002. Section 302 of Sarbanes-Oxley requires certain senior company leaders to indicate quarterly that they are personally familiar with internal systems and controls regarding [financial] reporting, operations, and compliance. Section 404 of Sarbanes-Oxley requires the financial auditor of publicly-traded companies to review and express a conclusion or opinion regarding internal controls of financial reporting. The COSO internal controls framework has been widely adopted for U.S. companies. The COSO internal control framework – as well as the COSO Enterprise Risk Management framework published in 2004 – is process-oriented.

Many internal controls involve IT systems: access rights, design of system, features, and outputs, to name a few. We will revisit this in Section 3 in the context of an IPSA.

The SEC Rule for conflict minerals is a new type of rule. Some laws, regulations, or accounting rules have affected environmental or similar non-financial matters. For example, companies with legally-enforceable requirements to clean up legacy contaminated properties must establish reserves for these contingent liabilities if they meet certain criteria. However, companies must establish reserves for any and all contingent liabilities – not just those associated with environmental contamination. Companies must disclose matters of material risk in Management Discussion & Analysis (MD&A) sections of

[3] See http://www.coso.org/

financial filing. The SEC issued an interpretive release in 2010[4] on how climate change should be considered for purposes of disclosure in financial filings. This release established nothing new for climate change, however; it simply explained SEC's existing criteria for risk-related disclosures. In fact, the SEC referenced other entities and reporting mechanisms[5] for more detailed information on companies' reporting of climate change-related information.

The conflict minerals rule is different. DFCM is arguably the first time that a social issue has been the primary driver for a rule related to financial reporting or disclosure. The SEC promulgated the rule, and is responsible for oversight. However, the disclosures related to company products, sourcing practices, and due diligence are not part of the income statement, the balance sheet, or other traditional elements of financial reporting. The very name of the form developed by the SEC – "Specialized Disclosure" – should be a tip-off that this is not a conventional filing. The SEC made several distinctions in the final rule between the Form SD and Conflict Minerals Report, and other aspects of financial reporting and disclosure.

The American Institute of Certified Public Accountants (AICPA) has published several FAQs related to conflict minerals. AICPA published FAQ 14 and 15 in January 2015[6]. The author suggests that the underlying issues driving these FAQs was the distinction between the conflict minerals reporting submittals and financial reporting and disclosures. Each one relates to data management in some way.

FAQ 15 confirms that testing of internal controls – required as part of assurance on financial reporting – is not part of an IPSA. Many internal controls involve controls designed into data management systems. Therefore, specialized IT resources and procedures need not be anticipated as part of an IPSA.

[4] See https://www.sec.gov/rules/interp/2010/33-9106.pdf

[5] SEC's interpretative guidance referenced the Carbon Disclosure Project (found at www.cdproject.net) and company-issued Sustainability reports, prepared using guidelines published by the Global Reporting Initiative (see www.globalreporting.org).

[6] See http://www.aicpa.org/InterestAreas/FRC/DownloadableDocuments/Conflict_Minerals/FRC_Conflict_Minerals_14_15.pdf.

FAQ 14[7] suggests that IPSA audit providers may wish to consider obtaining a management representation letter from the audit client. One such representation is that Management [of the auditee] has "disclosed to you all known control deficiencies, including significant deficiencies and material weaknesses, in the design or operation of our internal controls regarding the reliability and the preparation of the CMR and the related disclosures in the Form SD." Key elements the SEC disclosures - the CMR, in particular – are data-driven, and depend upon IT and data management systems. This representation implies that the public issuer has thought about the internal controls related to conflict minerals data.

The author suggests that the knowledge of these controls may reside in organizational groups that may be outside the core conflict minerals team. For example, an IT group may have designed a tool to manage conflict minerals data. Who determined what controls were required, and how those controls would be monitored – and revised, if necessary? If a vender were used, they likely have standard controls for the products and/or services they offer. Were these controls modified for the auditee? If so, how?

Even though FAQ 15 states that testing of internal controls is not part of the IPSA, the IPSA auditor will still expect the auditee to disclose known gaps in those internal controls – including those involving data management. If the auditee has not considered conflict minerals procedures in the context of internal controls and potential gaps, the IPSA Auditor may consider this in their risk assessment, and development of their audit plan.

3.3 Data Management and the IPSAs: Examples

IPSA procedures will inevitably encounter data, and the systems and controls for managing data and information, as the basis for statements in the CMR that relate to both audit objectives.

IPSA Objective #1 requires the auditor to draw a conclusion about consistency of the public issuer's due diligence program with the OECD Guidelines. The auditee can expect to describe the design of the due diligence program; this will undoubtedly include business processes and controls that are enabled by

[7] AICPA FAQ 14 begins with a reference to standards for attest engagements, which are to be used by CPAs in performing IPSAs. As a practical matter, the public issuer should expect that non-CPA IPSA auditors will adopt these practices as well. Indeed, in IPSAs conducted for the 2014 reporting year, at least one non-CPA auditor mentioned in their report that they had obtained a Management Representation letter.

technology. The auditee can expect to describe the controls embedded in IT systems, at least for those controls that are in place to ensure consistency with the OECD Guidelines.

IPSA Objective #2 requires the auditor to gain comfort over the veracity of statements describing steps taken for due diligence. Some example statements, and an IPSA auditor's considerations regarding data management are provided below.

"We consolidated supplier CMRTs to identify smelters in our supply chain."

The IPSA auditor may consider risks that the data management system was not designed to capture all of the supplier CMRTs, or if some fields of the CMRT were not incorporated in the consolidation.

"If we did not get a response from supplier in 30 days, we notified them again."

The IPSA auditor may consider risks that the design of data management system did not include this feature, or if it triggered at an interval longer than 30 days. If this feature were not designed as described, the reader of the CMR could assume the company performed diligence at a higher intensity than was actually done.

"We compared the supplier conflict minerals information (CMRTs) with our own criteria, and rejected CMRTs that did not meet our acceptability criteria."

This comparison could be done manually, or via an IT tool. The IPSA auditor may consider risks that the algorithm did not match the company's written acceptance criteria? For example, an IT vendor may have a default set of criteria, whereas the company has described stricter criteria in their CMR or internal procedures. If not supported, the reader of the CMR could assume that the issuer has implemented a degree of rigor that they did not.

"We incorporated conflict minerals training into supplier on-boarding process."

Supplier on-boarding is often managed in an enterprise-wide IT platform. Although this is a general statement, the IPSA auditor could consider risks that this provision was not embedded into all applicable suppliers. For example, a large company filing consolidated financial statements (and one CMR) may have several business units, each with their own procurement systems. As written, the statement implies that conflict minerals training has been incorporated into on-boarding processes for all applicable suppliers. The statement also mentions "training" – not "acknowledgment." Many training platforms are computer-based , and compile records on who completed training and when. The IPSA auditor may consider risks that some suppliers

have been overlooked, or that the applicable provision has not been designed into the supplier management platform as stated.

"We engaged an IT/ data management vendor to assist us with our conflict minerals program."

Several vendors have developed data management systems and tools that have been very helpful to companies overwhelmed by conflict minerals requirements. A purchase order or any correspondence supporting the company's engagement of such a vendor could be suitable support for this statement. Some vendors offer a "one-stop shop" of software and services; other vendors offer services as required; still others may only provide software or a tool. The author has noted that contracts involving software and services can pose distinct risks. The two contracting parties may have differing views of what services are in scope; these differences may not surface until some tasks are not performed and problems arise. The IPSA auditor, however, may consider the risk that some tasks have fallen between the cracks, and some other statements in the CMR may not be fully supported. The author suggests that IPSA auditees who use vendors for data management tools implement appropriate procedures and controls to ensure that all parties understand their roles and responsibilities. Furthermore, the public issuer should be prepared to provide suitable documentation to support a seamless working relationship with the vendor.

3.4 A Word About Fraud

We have witnessed a series of high-profile events where fraud has led, or been a very key contributor, to the downfall of once-respected companies, and substantial economic losses. Financial auditors must consider the potential for fraud. The International Professional Practices Framework (IPPF) published by the Institute of Internal Auditors states that internal auditors must exercise due professional care by considering fraud, and that "internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.[8]"

Fraud is most commonly associated with intentional misrepresentations in order to persuade another to give up money or other personal property. Fraud, however, can include any deception for the purpose of financial or personal gain.

[8] See IPPF Section 1220.A1 and Practice Advisory 2210.A2; available at https://na.theiia.org/standards-guidance/topics/Pages/Fraud.aspx

AICPA FAQ 14 includes a section whereby Management represents that:

> *"We have no knowledge of abuse, fraud, or suspected or alleged fraud affecting the Company involving:*
> - *Management*
> - *Employees who have significant roles in internal control over the preparation of the CMR or the related disclosures in the Form SD*
> - *Others where the fraud could have a material effect on the CMR or the related disclosures in the Form SD."*

How might this pertain to conflict minerals data management? One common enabler of fraud is access to information by unauthorized or inappropriate individuals. Insufficient restriction of access to data and information can result in unauthorized alteration of data that is relied upon for conclusions and reporting.

Data management systems hold the keys to the basis for public issuers' ability to make statements about the design of their due diligence framework, and for statements about the steps they took to implement due diligence. There should be controls to restrict access to appropriate parties. There could be risks that someone could override controls and change reports – for example, to hide the inclusion of a prohibited smelter or refiner in the supply chain, or to selectively (and inappropriately) draw from different data sets in order to support a desired conclusion.

The author notes that Question 6 in the Conflict Minerals Reporting Template[9] - the standard tool for collecting 3TG information from supply chains - asks whether "the company has identified all of the smelters your company and its suppliers used to supply the products included within the declaration scope?" Be ensuring that suppliers include all applicable smelters – not just those the customer may be looking for - this question has the effect of deterring fraud.

There will be many more discussions about fraud in the context of conflict minerals. Many of these discussions will involve data management. As public issuers prepare for IPSAs, they should think about how data management systems can enable and improve controls to ensure accurate, supportable information – and to prevent unauthorized tampering with this information.

[9] Developed by the Electronic Industry Citizenship Coalition the GeSI; available at http://www.conflictfreesourcing.org/conflict-minerals-reporting-template/

4.0 CLOSING COMMENTS

DFCM involves managing a considerable amount of data, much of which is new to organizations.

Data management is critical for reporting required by the SEC by Rule. This includes elements of the Conflict Minerals Report subject to the IPSA.

Conflict minerals reporting outside the scope of regulatory filings also involves information and data enabled via data management systems. The variety of information requested requires perhaps more robust controls to ensure that the right information – and only the appropriate information – is reported to stakeholders.

Companies affected by DFCM – either directly (as public issuers) or indirectly (as their suppliers) should design data management systems to generate data that is fit for intended purpose. The source and support for all data and info should be traceable.

Restrict access to data management systems to only those who need it, and to appropriate segments of the system. Consider how individuals could manipulate IT/ data management systems to hide unwanted information, or to yield info favorable to the organization or that individual. Implement controls that prevent such actions. Be prepared to identify what they are, and to demonstrate that they work.

If you engage a vendor for software and professional services, make sure that the roles and responsibilities are such that actions are seamless, and nothing falls between the cracks.

Look for all the ways that IT and data management systems can create a more efficient, effective conflict minerals program. Look for ways that this has enabled efficiencies in other areas. Where the investment in IT and data management systems IT has saved the company money, communicate this – at a minimum, to your company management. These stories don't tell themselves. Use IT/ DMS to create a more robust CM management program.

If you are considering an Independent Private Sector Audit, be prepared to discuss all the ways that IT and data management systems enable and support your due diligence program, the basis for steps you have reported in the Conflict Minerals Report, and the overall program. Be prepared to demonstrate that these systems are operating according to design.

ATTACHMENT: PROFESSIONAL EXPERIENCE

Mr. Douglas Hileman, CRMA, CPEA, P. E., QEP CPEA will be the project manager and primary contact for this effort. Mr. Hileman has nearly 40 years of experience in compliance, risk management, and auditing. He performed his first Environmental Audit in 1978, and has been involved in the field ever since. Mr. Hileman began working with internal audit and external audit functions in 2002, when he joined PricewaterhouseCoopers LLP.

Mr. Hileman led Independent Private Sector Audits (IPSAs) for a public issuer for the 2013 and 2014 reporting periods. He has conducted IPSA Readiness Assessments and limited Conflict Minerals Program assessments. He has provided advisory support on conflict minerals programs, and has developed business processes, internal controls, and training programs. He has supported the procurement of data management vendors, readiness assessments, and an IPSA for a client where his firm had independence conflicts.

He developed the website www.DFCMAudit.com as a resource for those interested in IPSAs, and has posted several white papers and tip sheets to the website. Mr. Hileman is a frequent contributor to industry group, professional group, and other firms' publications, webinars, and workshops on conflict minerals. His involvement with Dodd-Frank Conflict Minerals dates back to the comment period for the draft SEC rule. The final SEC rule references his comments several times.

Douglas Hileman Consulting LLC (DHC) has clients nationwide. The firm has built a network of experienced professional colleagues with credentials in several aspects of conflict minerals program assessments, including supporting IPSAs.

Mr. Hileman is on the Board of the Institute of Internal Auditors (IIA) Los Angeles Chapter. He has served on the (global) IIA Professional Issues Committee for three years. He has been on the Board of the [Environmental, Health & Safety] Auditing Roundtable. He has taught at UCLA Extension's Sustainability certificate program, focusing on Sustainability and financial and other reporting frameworks.