Checklist: Internal Controls for E & S Information

PracticalESG.com

Environmental and social (E & S) data and information is reported to regulators, investors, asset managers, NGOs, the public and ESG ratings agencies, yet it is frequently not subjected to adequate internal controls. Errors and omissions in the data perpetuate through the ESG information ecosystem, which is problematic. Therefore establishing internal controls for E & S data and its disclosure are necessary.

Some companies may have an Enterprise Risk Management (ERM) framework in place; they may find it efficient to add E & S into those processes. For example, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published October 2018 guidance: "Applying enterprise risk management to environmental, social and governance-related risks." However, for companies that currently don't use the COSO framework, this framework may be overwhelming and focuses on risk identification and management rather than on data quality, verification and reporting.

A company's internal control over financial reporting (ICFR) provides a good model for E & S information controls, especially for data that forms the basis of voluntary and required disclosures.

ICFR Generally

ICFR focuses on providing reasonable assurance that public reporting of information is reliable and prepared in accordance with generally accepted accounting principles (GAAP). In the E & S context, GAAP isn't applicable and unlike financial data, E & S data comes from a variety of sources, but generalized ICFR concepts are relevant. E & S information controls apply at a site level as well as to a corporate level. ICFR includes preventive and detective controls. Some activities fit in either category.

Developing and implementing ICFR controls for E & S

E & S professionals may not be familiar with the lexicon of "controls." The term "management systems" may resonate with them more and to a large extent embody the same concepts. If the company has implemented environmental, safety or responsible sourcing management systems such as

ISO or industry specific programs (e.g., Responsible Care for the chemical industry or ICMM's Mining Principles for the mining industry), those programs address many elements of ICFR. The existence of management systems can be considered preventive controls, while implementation of those systems may be both preventive and detective controls.

Use caution in relying on E & S management systems certifications issued to sites or the company as a control. There tend to be gaps between the existence of written procedures/program elements (what these certifications tend to focus on) and their implementation (which is much more important in the controls context). It is also common for E & S procedures in management systems frameworks to sit for long periods of time without being reviewed or updated – which is itself a gap in implementation of the system/controls.

Finally, it is important to remember that fraud in E & S information is a relevant risk, so controls should be developed and implement with that in mind. Typical E & S management systems tend to discount the potential for fraud.

Who should be involved in development & implementing controls?

As with other aspects of E & S, the development and implementation of internal controls benefits from a multi-functional perspective. When developing and implementing these controls, companies should strive to engage participants in departments/functions including:

Role/function	Controls perspective
Executives	Policies, communications, financial management,
Management	Policies, enforcement, communications, culture, financial management,
Operations/production staff	Physical equipment controls, practical implementation of policies, communications, culture, training, procedures, data management, documentation, monitoring systems and corrective action implementation
Maintenance department	Physical equipment controls, communications, culture, training, procedures, data management, documentation, monitoring systems and corrective action implementation
EHS/sustainability staff	Physical equipment controls, communications, culture, training, procedures, data management, documentation, regulatory management, monitoring systems and corrective action implementation

Engineering/R&D	Communications, culture, training, procedures, data management, documentation, regulatory management, supplier management, materials specifications, monitoring systems and corrective action implementation
Procurement/purchasing department	Supplier management, administrative controls, financial management, communications, culture, training, data management, materials specifications
Accounting department	Policies, enforcement, administrative controls, procedures, communications, culture, training, data management, documentation, financial management,
Internal audit	Physical equipment controls, administrative controls, procedures, financial management, communications, culture, training, data management, regulatory management, monitoring systems and corrective action implementation
Risk Management department	Policies, physical equipment controls, administrative controls, communications, culture, documentation, monitoring systems and corrective action implementation
Legal department	Policies, communications, administrative controls, regulatory management, data management, monitoring, documentation
Training staff	Policies, culture, training, data management, documentation
IT staff	Data management, data security, monitoring systems and corrective action implementation

Preventive controls

Preventive controls are intended to deter and prevent E & S data errors or fraud from happening to begin with. Generally speaking, these involve developing and implementing procedures and include documentation, physical process controls and equipment and authorization/review practices. Separation of duties, a key part of authorization and review practices, ensures that no single individual is in a position to both (a) authorize/review/approve, and (b) be responsible for executing the activity requiring that authorization/review/approval.

It is important to consider that controls are especially critical for non-routine events. Emergency situations, shutdowns, maintenance outages, worker strikes and supply chain disruptions are site conditions where controls can be side stepped while pursuing speedy business recovery.

A non-exhaustive list of examples of preventive controls for E & S data at operating locations includes:

- Establishing a site-level policy for E & S operating expectations that are consistent with corporate mandates. Confirm that site management is aware of and understands these expectations.

- Establishing a supplier code of conduct or similar expectations that are consistent with corporate mandates.

- Establishing business integrity policies and procedures prohibiting bribery, corruption, fraud, abuse and harassment.

- Establishing site-level E & S committees. A site may have separate environmental, health and safety committees, or a combined EHS committee.

- Formally assigning E & S job responsibilities to employees, including backups/alternates in the event of employee illness, injury or vacations. All relevant employees should understand these job responsibilities.

- Establishing formal written job-specific personnel performance metrics specific to E & S as part of annual performance evaluations. All relevant employees should understand these performance metrics and they should be consistent with corporate mandates.

- Developing and posting formal written operating procedures for equipment and inspections. These should be available in all languages relevant to the workforce at the location(s) and consistent with corporate mandates.

- Providing on-going job specific and company general employee training on E & S topics consistent with corporate mandates.

- Establish formal communication procedures for E & S events such as injuries, emergencies, government site inspections.

- Establish formal written procedures for advance review and approval of E & S data that is submitted to regulatory authorities.

- Management enforcement of conformance to policies, procedures and performance requirements through a system of incentives and disincentives, up to termination of employment. This should be done consistent with corporate mandates.

- Developing and supporting peer-to-peer enforcement of E & S standards (corporate culture).
- Providing an anonymous mechanism for internal reporting of E & S concerns (hotline).
- Implement a “no retaliation” policy for employees who report their concerns. This should be done consistent with corporate mandates.
- Developing E & S risk/legal requirements registries and ensure they are reviewed and updated regularly.
- Developing E & S regulatory compliance and reporting calendars and ensure they are reviewed and updated regularly.
- Requiring written EHS signoff in advance of implementing operational changes (such as obtaining new chemicals, increasing production, modifying equipment, new products or new construction).
- Limiting physical access to equipment or facility areas as part of safety measures. This may include physical or administrative controls. This should be done consistent with corporate mandates.
- Ensuring pollution control sampling/monitoring and safety equipment is tested, operated, maintained and calibrated in accordance with manufacturer specifications.
- Minimizing opportunities for E & S data transcription errors (i.e., maximize use of auto logged data)
- Implementing real time or daily tracking/logging of operating conditions, output, chemical use, fuel use, etc.
- Implementing automated chemical inventory management systems, linked to chemical vendors.
- Reviewing EHS operating procedures for all contractors/vendors working on site to ensure they have adequate training and procedures consistent with the site and corporate requirements.

- Conducting new supplier due diligence for environmental impacts, employee workplace conditions and wages and conformance to corporate standards.

- Ensuring supplier contracts or PO terms and conditions include a reservation of audit rights clause.

- Providing training to suppliers and contractors on E & S requirements of the company/location.

- When using external auditors/industry programs for E & S data and/or certifications for E & S statements, conduct formal due diligence on the auditors and certification mechanisms to ensure they are credible, professional and worthy of reliance. In particular, evaluate the auditors' technical competence and their processes for corroborating information from interviews.

- Reviewing worker safety, working conditions, pay programs and incident reports/reporting procedures to ensure they cover seasonal, migrant, temporary and contract workers.

- Confirming that, where appropriate, documented programs and procedures aligned with ILO Conventions are established.

- Minimizing staff access to E & S data and authority for changing it.

Detective controls.

Detective controls are designed to catch items, topics or events that have been missed by preventive controls. Once identified, those items can be corrected. Detective controls revolve around data reconciliation and confirmation. This is typically where fraud would be detected if it has occurred.

A non-exhaustive list of examples of detective controls for E & S data at operating locations includes:

- Regular reporting of monitoring results, challenges/problems to management (i.e., at the site level, daily operations meetings). Quarterly dashboards can also be created for the full board or a specific committee overseeing E&S strategies.

- Maintaining adequate documentation (written or electronic) of all E & S matters consistent with corporate mandates and legal frameworks such as Attorney-Client Privilege.

- Following a segregation of duties framework, review manual activity/inspection logs for completeness of schedule and activities, as well as confirm dates logged are consistent with operating and employee work schedules (i.e., no “pencil whipping” or pre-completed forms are used).

- Following a segregation of duties framework, review approvals/signoff documents to ensure they are complete and properly signed/dated (i.e., no “pencil whipping” or pre-signed blank forms are used).

- Conducting periodic reviews of E & S spreadsheet formulas for modifications, confirm calculations are correct and correct data is in the right cells.

- Conducting regular site inspections of all facility areas, using different staff to obtain different perspectives of site conditions and activities.

- Conducting periodic E & S audits, either internal or external. Audits conducted by customers may be considered an internal control only where results are made available to the site/company.

- Confirming reported stored and used volumes of chemicals, wastes and safety equipment by performing periodic reconciliations of inventory and purchasing/disposal records.

- Performing manual reviews and checks of supplier responses to information requests (ground truth against internal expertise/expectations). Responses that are inconsistent with internal expertise/expectations should be flagged for follow up and correction with the supplier.

- Monitoring existing suppliers for continuing conformance to corporate E & S standards and Codes of Conduct. If engaging external auditors, ensure the auditors have adequate qualifications to perform the audits to a level that is credible and reliable to warrant reliance.

- Monitoring industry supply chain due diligence mechanisms or ESG/sustainability certifications to confirm they remain credible and reliable to warrant reliance.

- Conducting periodic independent laboratory testing of materials, products and components obtained from suppliers to ensure they are consistent with site and corporate mandates (i.e., do not contain banned chemicals).

- Comparing documents provided by the site to known authentic examples (e.g., invoices, shipping documents, regulatory approvals/correspondence, signatures).

- Reviewing accident/incident investigation reports to verify the number and type of incidents reported. The site's conclusions, determinations and implementation of corrective actions should also be confirmed.

- Confirming that reported E & S data/information concerning workers includes seasonal, migrant, temporary and contract workers. Site injury/incident logs, reports and investigations should also cover seasonal, migrant, temporary and contract workers,

- Confirming that worker regular and overtime hours are accurately recorded and reported.

- Confirming that worker wage structures and leave/vacation at operating locations conform to local and national laws and company policies.

- Identifying conditions or situations where bypassing controls is allowable or has occurred and investigate the reasoning/cause. Corrective actions should be implemented to prevent bypassing of internal E & S data controls.

Corporate disclosure controls

Site-level controls as described above focus on providing reasonable assurance that E & S data at its point of generation does not contain meaningful errors and omissions. That data is frequently then aggregated at the corporate level and reported publicly. Additional ICFR controls are

appropriate to provide reasonable assurance that meaningful errors and omissions do not occur when publicly reporting that validated E & S data.

Once E & S data controls are in place and the data confirmed, disclosure controls may be less comprehensive and concentrate on verifying that errors and omissions are not in the report language or from transcribing already-verified data into the draft report. These include:

- Comparing E & S data and information included in draft disclosures to the applicable original internally provided information sources to ensure consistency (i.e., no transcription errors).
- Reviewing the original E&S data and information to confirm that disclosures are not misleading or cherry-picking.
- Confirming mathematical formulas and calculation results of verified data aggregated from multiple locations/sources (e.g., confirm spreadsheets are calculating correctly, capture all appropriate cells, cell values are correct and appropriate – no text in numerical cells)
- Using internal or external subject matter experts to review draft disclosures for technical accuracy.
- Conducting internal audits of draft disclosures, not just document reviews.
- Setting up escalation processes so management and legal can be aware of any disclosure errors and omissions without undue delay.
- Having the preparers of the E & S data and those in charge of disclosure controls certify to management and/or board directors of disclosure accuracy.

Gaps in data versus weakness in controls - terminology

In addition to potential issues with E & S data, deficiencies may be identified in the controls systems themselves. ICFR audits/assessments use terminology of “material weakness”, “significant deficiency”, and “deficiency.” As indicated in the introductory information, E & S professionals are likely more familiar with the lexicon of management systems - terminology like “major”, “minor”, “conformance”, “nonconformance”, “gap” and “finding.” It may be optimal to use different

terminology when discussing data versus the controls to ensure clarity. Getting alignment on terms and definitions is important to ensure there is consistency in understanding severity of identified deficiencies and prioritization for corrective actions.