TX Office: (817) 416-6842
NV Office: (702) 565-2727

Kral Ussery
Certified Public Accountants
Advisors - Litigation Support - Internal Audit

April 20, 2023

Data Quality and Information Flow

Leveraging Principle 13 of COSO's *Internal Control—Integrated Framework*

By Ron Kral, CPA, CMA, CGMA
Partner of Kral Ussery LLC

While there are many factors that determine organizational success, data quality and information flows are arguably two of the most important variables. Unfortunately, too many business decisions are made with incomplete or inaccurate information, or even worse, a lack of timely data thus precluding awareness of lurking risks and potential opportunities. As a result, faulty data and inadequate information flows can quickly throw an organization's decision-making process into chaos resulting in the destruction of shareholder value.

Fortunately, a powerful framework exists to help companies achieve their objectives and you have likely heard of it - the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) 2013 *Internal Control—Integrated Framework* (Framework). While implementing any of the 17 Principles can be daunting (refer to the Framework's Executive Summary for descriptions), this article explores the guidance from this Framework and implementation considerations for Principle 13 regarding quality information. But first, let's visit some general risks regarding information flows, as well as the distinction between the terms 'information' and 'data'.

Information versus Data

Collective knowledge feeding into the decision-making process is a critical success factor, thus posing big risks to organizations. Why? – because information is by definition biased. Essentially, information is data that is 'value-added' through analysis, interpretation, assumptions, conclusions, and presentations; whereas, 'data' constitutes raw-factual figures and details that can be electronically stored. Think of 'data' as the smallest units of factual information that can be used as a basis for calculations and discussions. Information is then the result of processing data for dissemination as a basis for taking action. Thus lies the risks in terms of who is harvesting and interpreting the data, and for what purposes. It is human nature to present data in the best possible light by the person(s) presenting it, or otherwise skewed to meet preconceived objectives. Whether it is a vendor making a pitch for business or the CEO arguing a position to the board, a lack of quality data and objective information is often a reality.

Data is the foundation of business performance thus enabling information, analytics, and artificial intelligence (AI). While it is mostly viewed as an intangible asset, although not often on the balance sheet, it can also be a liability. Dr. Prashanth Southekal identifies in his book, *Data Quality – Empowering Businesses with Analytics and AI,* four common scenarios where data can become a liability:

1. *Collecting data without a defined business purpose will result in huge data volumes, ultimately resulting in increased complexity and cost due to data management.*
2. *Data takes up vast amounts of energy to store, secure, and process, resulting in an increase in the carbon footprint for the business.*
3. *Cybercriminals are drawn to organizations that have large volumes of data.*
4. *Managing data also entails privacy compliance.*[1]

Organizations should seek to acquire complete, accurate, timely, and relevant data and information that is impartial without the taints of vested interests. Relying too heavily on a single source or two can prove catastrophic. This is where a robust internal audit function can pay dividends in helping to ensure that the data and information feeding into the decision-making process is adequate and objective. The board of directors needs to be comfortable with the information, including supporting data and assumptions. Executive management teams and their boards must work together to be confident with independent fact-checking activities. They need to understand that utilizing quality data and objective information is for the ultimate good of organizational value. This is where a skilled internal audit function can come into play.

Understanding Principle 13

Principle 13 of COSO's Framework reads[2]:

> ***The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.***

The Framework defines the following points of focus highlighting the important characteristics to this principle:

- *Identifies Information Requirements — A process is in place to identify the information required and expected to support the functioning of the other components of internal control and the achievement of the entity's objectives.*
- *Captures Internal and External Sources of Data — Information systems capture internal and external sources of data.*
- *Processes Relevant Data into Information — Information systems process and transform relevant data into information.*
- *Maintains Quality throughout Processing — Information systems produce information that is timely, current, accurate, complete, accessible, protected, and verifiable and retained. Information is reviewed to assess its relevance in supporting the internal control components.*
- *Considers Costs and Benefits — The nature, quantity, and precision of information communicated are commensurate with and support the achievement of objectives.*

While all five of these points of focus are critical in defining the spirit of Principle 13, it is the fourth one addressing 'quality' that is perhaps the most challenging. The Framework states that the quality of information depends on whether it is:

- *Accessible — The information is easy to obtain by those who need it. Users know what information is available and where in the information system that information is accessible.*

[1] Dr. Prashanth Southekal (2023), Data Quality – Empowering Businesses with Analytics and AI, published by Wiley.
[2] All quotes from the COSO *Internal Control—Integrated Framework* used by permission through Copyright-Permissions@aicpa-cima.com.

- *Correct — The underlying data is accurate and complete. Information systems include validation checks that address accuracy and completeness, including necessary exception resolution procedures.*
- *Current — The data gathered is from current sources and is gathered at the frequency needed.*
- *Protected — Access to sensitive information is restricted to authorized personnel. Data categorization (for example, confidential and top secret) supports information protection.*
- *Retained — Information is available over an extended period of time to support inquiries and inspections by external parties.*
- *Sufficient — There is enough information at the right level of detail relevant to information requirements. Extraneous data is eliminated to avoid inefficiency, misuse, or misinterpretation.*
- *Timely — The information is available from the information system when needed. Timely information helps with the early identification of events, trends, and issues.*
- *Valid — Information is obtained from authorized sources, gathered according to prescribed procedures, and represents events that actually occurred.*
- *Verifiable — Information is supported by evidence from the source. Management establishes information management policies with clear responsibility and accountability for the quality of the information.*

Relevance of Principle 13 to Financial Statements

While Principle 13 has long been one of my favorite Framework principles (refer to Three Challenging Principles to COSO's 2013 Framework from November 12, 2014), regulators are also paying attention. The Public Company Accounting Oversight Board (PCAOB) continues to challenge audit firms on how they became comfortable that their clients maintained quality data and information throughout the processing of it into the financial statements. This is especially common where information flows pass through multiple automated systems before the numbers make it to the general ledger. Here are some specific findings of the PCAOB as communicated in publicly available inspection reports:

- *The firm selected for testing a control over the monitoring of the transfer of data from the teller system to the general ledger. The firm did not evaluate whether the control was designed to address the risk related to the completeness of the data transferred.*[3]
- *The firm used certain participant data in its substantive testing of participant distributions. For a sample of participants selected for testing, the firm did not sufficiently test the accuracy of certain of the data because it limited its procedures to comparing the data from one system to another system. In addition, the firm did not test, or in the alternative, test any controls over, the completeness of the system-generated reports used to make its selections for testing certain participant data.*[4]

The U.S. Securities and Exchange Commission (SEC) also persistent in issuing comment letters to public entities questioning the application of US GAAP, including assumptions. While the comments generally do not explicitly cite a concern over data quality, the root cause for many of them are directly tied to Principle 13 in questioning the support of quality information in being correct, sufficient, timely, valid, or verifiable.

[3] Page 17, Crowe LLP, PCAOB Release No. 104-2023-002, November 16, 2022.
[4] Page 7, Mayer Hoffman McCann P.C., PCAOB Release No. 104-2022-200, September 15, 2022.

Implementation Considerations

Similar to all Framework principles, there is no single recipe for success as it depends on the industry, size, operating characteristics, and associated risks of the organization in customizing an effective approach. However, here are some ideas for generating and using relevant, quality information:

1. Understand and practice the full definition of 'governance'. While there are many definitions afloat, I define it as:

   > Governance is the decision-making process of directing, managing, and monitoring an organization with the goal of protecting and growing shareholder value while also taking into consideration the interests of key stakeholders such as customers, communities, competitors, creditors, employees, governments, investors, suppliers, and regulators.

   Addressing only part of this definition will likely leave organizations vulnerable to those that exercise the full definition. Understand that the 'decision-making process' rests on the quality of data and information flows. Organizations must clearly define the roles at the board, management, and internal audit levels to hold them accountable. While enhancing shareholder value is often a business objective, it is also important to keep in mind the stakeholder groups that are relied upon for success or can influence success. Take the time to truly understand them and their objectives in creating win-win strategies for those you rely upon. These insights will pave the way to harvesting the right data and information needed for robust decision-making.

2. Leverage the COSO Framework in achieving operating, reporting, and compliance objectives. This includes Principle 13 and its associated points of focus. While the Framework's points of focus are strictly a starting point for management in designing and implementing controls, they are reflective of the Principle characteristics. For Principle 13, here are some implementation ideas for each of the five points of focus:

   - Identifies Information Requirements: Revert back to the definition of governance to identify information needs by periodically asking the following questions:
     - What will be needed in support of board members, management teams, and auditors?
     - How do we define 'success' through KPIs and other metrics, and how do we benchmark to these definitions?
     - What is needed to understand the opportunities and risks of protecting and growing shareholder value in a timely manner?
     - What is the interest of stakeholder groups and what is needed to keep within their good graces?
   - Captures Internal and External Sources of Data: Data should be gathered from a variety of trustworthy sources, both internally and externally. The quality of the data should be verified and tested to ensure that it can be relied upon.
   - Processes Relevant Data into Information: Identifying, harvesting, processing storing, and destroying data can be costly. Therefore, it is important to have it properly identified, captured, and classified per the previous two points of focus. Management will need to develop and implement control activities to ensure data relevancy and that biases do not creep into the interpretation of data as it is transformed into information. Afterall, the decision maker should be basing their

decision on a combination of data elements and information that is relevant and trustworthy, meaning it does not unduly sway the decision one way or the other without credible support.

- Maintains Quality throughout Processing: Assign each of the elements that define 'quality' to a control owner(s) to ensure that each assertion is being met. Since there are nine such elements, this is easier said than done as no single control owner or department will likely own them all. In fact, it will take multiple functions and control owners to cover all of the quality assertions. For example, it is the user group (generally the controllership function when dealing with internal control over financial reporting – ICFR) who is requesting and using the data. They are instrumental in defining accessibility, sufficiency, validity, and that it is current. The information technology department (IT) will likely be ensuring that it is protected and available from the information system when needed (i.e., timely). The legal department generally oversees retention through a records retention policy and internal audit may also take a lead role in independently ensuring correctness and that the information is obtained from authorized sources (i.e., valid). Of course, internal audit may also help with other assertions such as confirming that the data is accurate and complete (i.e., correct), as well as all other elements are present and functioning. See the table below for typical responsibilities:

Quality of Info Elements per COSO Principle 13	Typical Lead Control Owning Department	Notes
Accessible	User Group (UG)	UG sets user access parameters and works with SaaS vendor and/or IT to ensure proper access
Correct	UG & IT	The UG is primarily responsible as the first line of defense, but also works with SaaS vendor and/or IT for validation checks. Internal Audit to verify
Current	UG	The UG is primarily responsible as the first line of defense, but also depends on who is gathering info
Protected	IT	UG and Legal also responsible for helping to define data categorization
Retained	Legal & IT	Legal is responsible for policy and IT implements
Sufficient	UG	UG takes first crack with Executive Mngt, Legal, the Board, and Internal Audit also weighing-in
Timely	IT	SaaS vendor when applicable
Valid	UG	Internal Audit in confirming authorized sources
Verifiable	Executive Mngt.	Strong tone-at-the-top is important in enforcing policies on accountabilities

- Considers Costs and Benefits: Of course, the above control activities cost money that must be carefully balanced against the expected benefits. This must be constantly monitored and re-evaluated to ensure that resources are properly aligned with results.

3. Ensure there are adequate data quality and information flow controls (i.e., policies and procedures) and that these controls are present and functioning within a process to mitigate risks and take advantages of opportunities. Remember that controls exhaust resources so it is important to select a balance of control types that best protects and grows shareholder value.

Conclusion

Principle 13 can be daunting for companies and auditors alike as it encompasses capturing and processing relevant information, as well as maintaining quality throughout the process. For financial reporting purposes, this culminate in the preparation and audit of financial statements in accordance with US GAAP and SEC Regulation S-X if an SEC registrant. Quality information means that it is accessible, correct, current, protected, retained, sufficient, timely, valid, and verifiable per the Framework. Since many financial reporting control owners and auditors do not have data quality and related IT backgrounds, these areas are likely outside their comfort zones. Hence, the need for deeper data quality and information flow skills is essential in implementing Principle 13. A good starting point is to undertake an independent risk assessment of your data environment to assess organizational maturity, roles, and to identify risks and opportunities.

*****

Ron Kral is a partner of Kral Ussery LLC, a public accounting firm delivering SEC and accounting advisory services, litigation support, and internal audits. Ron is a highly rated speaker, trainer, and advisor. He is a member of 4 of the 5 COSO sponsoring organizations; the AICPA, FEI, IIA, and IMA. Contact Ron at Rkral@KralUssery.com or www.linkedin.com/in/ronkral.

Kral Ussery LLC is a public accounting firm delivering advisory services, litigation support and internal audits. We serve U.S. public and private companies to protect and grow shareholder value, as well as non-profits and governments on internal controls and combating fraud. Our firm assists entities in all matters relating to financial reporting, including SEC compliance, internal controls, SOX-404, IT general controls, IPO readiness, M&A transactions, US GAAP compliance, audit preparedness, and internal auditing. Visit us at www.KralUssery.com.

This is an article from the Governance Issues™ Newsletter, Volume 2023, Number 2, published on April 20, 2023, by Kral Ussery LLC.