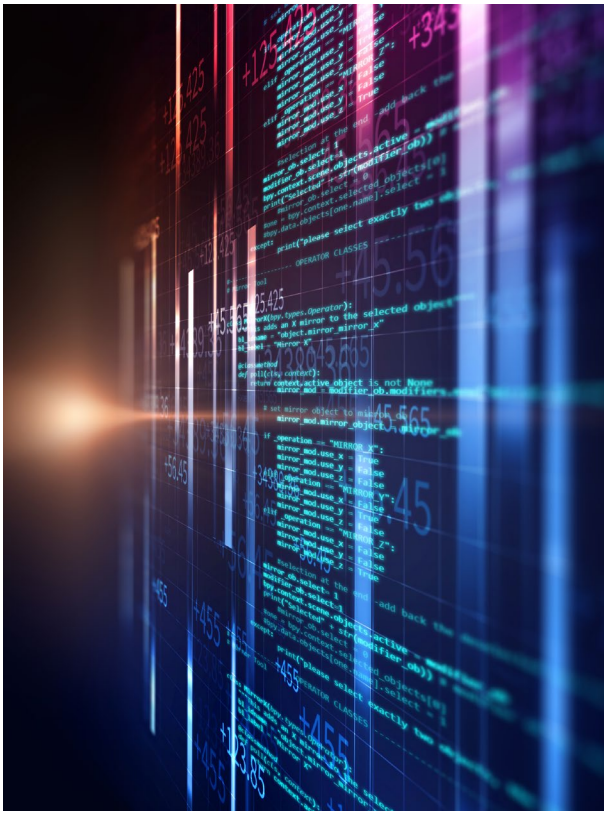
Point of View

5 Steps to Clean Data and Reduce Risk

Why is clean data important? It drives all well-informed business decisions. Likewise, bad data may lead to bad business decisions. In financial crime risk management and detection, accurate data that cannot be manipulated is crucial to preventing financial crime. If your fraud or anti-money laundering (AML) program is undermined by poor data, then you are vulnerable to reputational harm, enforcement action and liability.



Consider these statistics:

- Poor data quality costs the U.S. economy $3.1 trillion per year, according to IBM
- The estimated amount of money laundered globally in one year is 2 to 5 percent of global gross domestic product, or $800 billion to $2 trillion, according to the United Nations Office on Drugs and Crime
- U.S. authorities have levied $17 billion in money laundering penalties since 2009, according to Quinlan & Associates

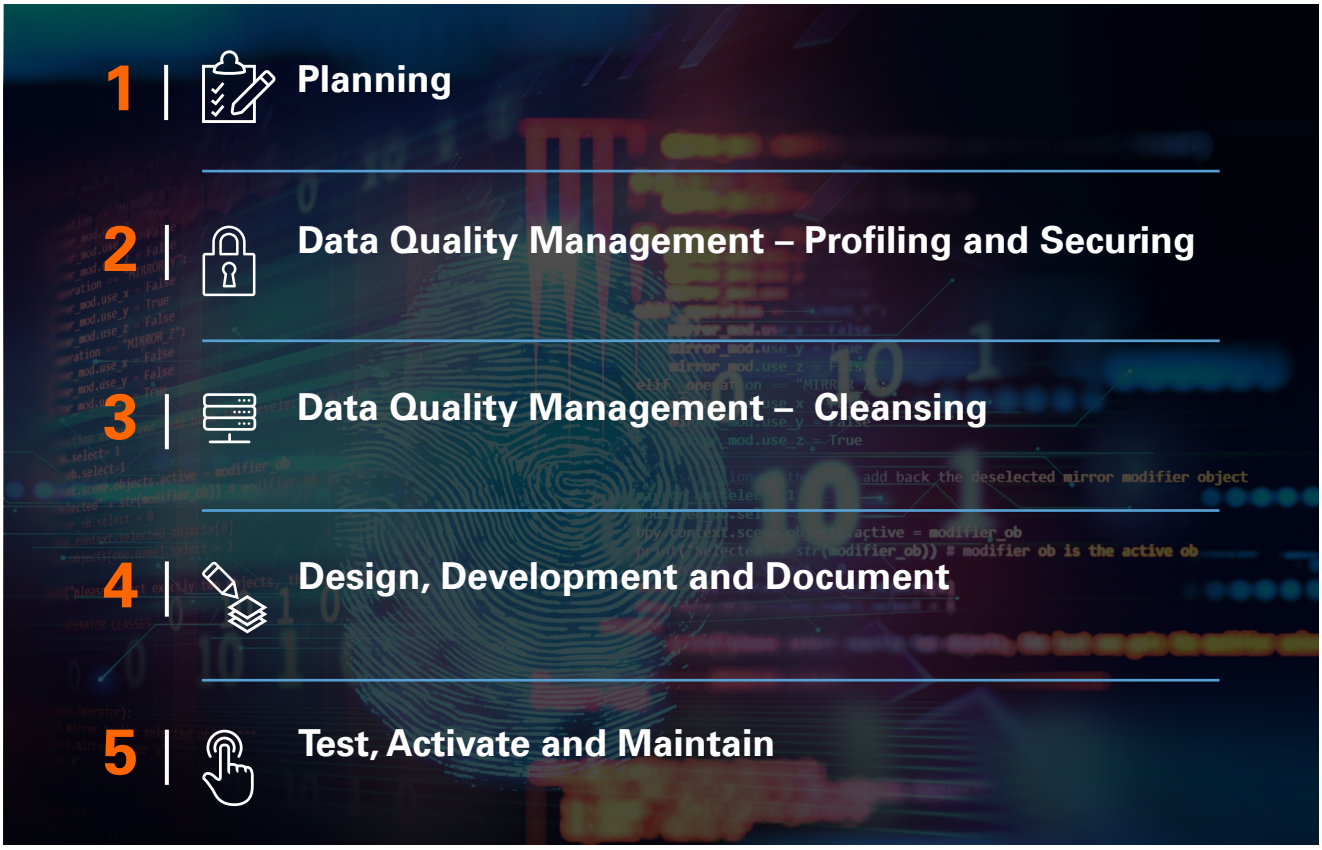
Clean data is about more than accuracy. It involves monitoring and maintaining the data (including origins and changes) over its life cycle. Consider these three areas to help ensure clean data:

- **Data Accuracy –** Ensuring the data's veracity
- **Data Consistency –** Maintaining the integrity of data over its life cycle
- **Data Life Cycle –** Monitoring data origins and changes throughout the data life cycle (also called data lineage)

Understanding and validating data allows for transparent governance, which mitigates professional and personal liability and easily identifies deliberate manipulation of data to circumvent detection. Auditors, stakeholders, customers and staff members all need a clear understanding of the data source and validity so they can trust the data underlying the reporting of fraud, money laundering and other financial crimes.

Follow this five-step process to protect data accuracy, consistency and lineage:

5 Steps You Can Take to protect data accuracy, consistency and lineage



Step 1: Planning

- Document objectives by defining and understanding the risks that you need to assess
- Choose the right data-detection techniques, such as behavioral analytics for suspicious activity detection, real-time fuzzy text matching for sanction screening and real-time inference for unusual payment activity
- Identify data sources and limitations and plan how to enrich your data
- Document your plan and define each risk along the way, including where data comes from and whether you need to see all of it or just changes

Step 2: Data Quality Management – Profiling and Securing

- Identify and normalize the data
  - Make sure it's in the right format, such as addresses
  - Modify and reconcile the data by, for example, having ISO codes and country descriptions
- Use third-party data, such as from Dun & Bradstreet or Dow Jones, to enhance your own
- Secure data to ensure it is not compromised:
  - Have dedicated landing zones for the data
  - Use end-to-end encryption hardware and software
  - Retain and reconcile data

Step 3: Data Quality Management – Cleansing

- Identify exclusions, such as fees from ATM charges, or institution-initiated transactions, such as interest payments
- Make sure you are de-duping multiple sources of the same transactions and overlapping data
- Ensure the appropriate controls, making sure all data is included, and if data is excluded, document why

Step 4: Design, Develop and Document

- Adopt a risk-based approach to data and prioritize based on risk type
- Document the flow of your data based on multiple transaction cycles
- Create rules that define default values for missing data and input hierarchies
- Create a detailed verification report with automated notifications and escalations
- Provide proof of data origins and changes throughout the data life cycle
- Clearly understand and document limitations or requirements placed on the data from the source (starting point) or the system (end point)

Step 5: Test, Activate and Maintain

- Implement a process to reconcile your data, including creating test scripts. Review the accuracy and precision of data and run ongoing balancing reports
- Establish a change control process to cover new sources or newly collected data, such as new products and service data, and keep current with regulations
- Review your alerts and map back to the source system to prepare for potential regulator questions
- Continually enhance your program with governance review, data mapping and model validation

Once your plan is in place, make sure you have a robust and flexible data integration architecture in your fraud and AML solutions to accommodate the program requirements. The solutions should provide secure data transmission, secure record-keeping and a method for data reconciling, anomaly detection and reporting.

Developing and implementing a plan to support data accuracy, consistency and life cycle as part of your financial crime risk management program will help ensure risk detection and mitigation, regulatory compliance and protection from reputational harm. Your plan should not be a static document, but rather a dynamic data plan that changes when you bring in a new product or new data.

Connect With Us

For more information about AML technologies, call 800-872-7882, email getsolutions@fiserv.com or visit fiserv.com.

Fiserv is driving innovation in Payments, Processing Services, Risk & Compliance, Customer & Channel Management and Insights & Optimising. Our solutions help clients deliver financial services at the speed of life to enhance the way people live and work today. Visit fiserv.com to learn more.

Fiserv, Inc.
255 Fiserv Drive
Brookfield, WI 53045

800-872-7882
262-879-5322
getsolutions@fiserv.com
www.fiserv.com

199665-COL 10/18