4 Steps to Leveraging SAP Data for Compliance Analytics

Case IQ

Introduction

Is your organization looking for ways to leverage your SAP data to mitigate compliance risks and stay ahead of potential issues? In this white paper, we'll cover how to take advantage of the comprehensive and structured information in your SAP ERP by leveraging compliance data analytics to identify anomalous transactions that may indicate fraud, bribery, corruption, embezzlement, asset misappropriation, conflicts of interest or sanctions violations. These four steps can help your organization detect non-compliance before it becomes systemic and continuously improve your compliance program to make it as effective as possible.

SAP ERP is an enterprise resource planning software developed by the German company SAP SE and used by ninety-nine of one hundred of the world's largest companies. The most popular SAP ERP products are SAP ECC, S/4 Hana, and SAP Business One.

SAP ERP data contains comprehensive and structured information that can help identify patterns and anomalies that can be indicative of compliance risks or failures. For example, data within SAP can be used to identify violations of anti-corruption laws such as the Foreign potential risks across the enterprise holistically and can empower compliance to investigate possible non-compliance and respond quickly to emerging compliance issues. Leveraging SAP data also enables compliance teams to trace data back to its source, so that they can examine the processes used to extract the data and identify if data has been altered or manipulated.

Using SAP data for compliance data analytics provides organizations with robust data to mitigate compliance risks and can help companies stay compliant with regulations and identify issues before they become critical problems. There are a variety of steps that companies should take to leverage their SAP data. This white paper will review these considerations and the methods of leveraging SAP data to empower compliance data analytics and reduce risk.

1. Understand Your ERP Instances

ERPs are typically large and complex software systems that require a robust IT infrastructure to support them, including software tools such as databases, middleware, and development environments. Start by investigating how many SAP instances are used by your organization. The IT team should have this information readily available. Do a completeness check against the list of legal entities to ensure you have a full mapping of SAP instances across your entities. Quite often, a small legal entity that uses a less common non-SAP ERP to track its transactions gets overlooked. Once you know the landscape, determine the priority of your monitoring efforts. For example, you may choose to prioritize a smaller SAP instance if it covers higher-risk countries and deprioritize a larger instance covering a larger but historically lower-risk market.

Controls:

ERPs are designed to streamline and automate business processes across different departments, such as finance, sales, procurement, human resources, and more. Understanding the organization's business processes, interdependencies, and how they are integrated with the ERP system is essential.

Some areas to investigate within the ERP system include:

- Vendor and customer management: Ensure that all vendors and customers are recorded in the SAP vendor and customer master files and identify any high-risk classifications in SAP.
- Due diligence results: Assess whether any information from your third-party due diligence process is being recorded in your SAP data, such as the third party's due diligence completion status, risk levels or level of government interaction.
- Automated controls for supply chain management: Look into purchase requisitions (PRs), purchase orders (POs), and invoices without POs and understand how they relate to your SAP data (i.e., are these steps managed within SAP or partially or fully outside of SAP).
- Three-way matching process: Assess the system's ability to perform three-way matching prior to payment.
- Automated workflows: Confirm that pricing adjustments and credit notes have automated workflows in place.
- Separate security roles: Ensure that distinct security roles exist for individuals who can create customers/vendors and those who can create orders or POs, respectively.

Relevant Data:

Identification of compliance risks using data analytics within your SAP data will require multiple data points within that data. For example, master data on your vendors, customers, and employees can be used to identify potential conflicts of interest, wherein names and addresses of parties can match and show unusual relationships.

Financial transaction data such as vendor payments, invoices, and purchase orders will provide the most value in terms of helping to identify potential non-compliance, such as bribery or kickback schemes.

Organizations can detect potential corruption by analyzing transaction patterns and identifying suspicious payments. The key to conducting efficient monitoring will be connecting the PRs, POs, Invoices, and Payments. There are simplistic approaches that look at each document in isolation, but those approaches miss many risks and result in a multiplication of review work, requiring review of the same transaction multiple times. The more powerful approach is to connect data across the payment lifecycle and review that transaction holistically once.

The key to gathering the relevant data will be to connect all relevant SAP tables to extract the information you need to analyze. For example, vendor bank information is found in LFBK while master vendor general information is in ADRC, LFA1, and LFB1. A strong partner will typically have SAP expertise and tooling (see Automating Your Data Acquisition below) that already defines the right tables to extract.

Other Data Outside of SAP:

Compliance data such as training records and investigations and policy violation data can help identify areas of the organization that may be at higher risk of non-compliance. For example, if a particular department has a high rate of policy violations, it may be a sign of a culture of non-compliance that could lead to issues like corruption.

Audit data, including internal and external audit reports, can provide valuable insights into potential areas of corruption risk. Organizations can detect potential corruption by analyzing audit findings and identifying patterns of non-compliance or questionable practices. Your data analytics process should allow for you to easily input factors from this data into your risk scoring methodology, ideally without needing to code or manipulate SQL or any other analytics coding language.

2. Automating Your Data Acquisition

Data will need to be received and prepared for analysis from SAP on a daily basis and tools exist to manage this automation. These tools can help organizations automate data acquisition by integrating data from various sources and processing it efficiently. However, large data sets can become unwieldy if you don't have a process to accumulate the data over time (or reprocess that data) in an organized manner.

As an example, procurement transactions have a significant breadth of data. Hypothetically, a small company with 500 employees might issue 500 purchase orders per month with an average of 10 line items per purchase order. So, even a small company could be producing 500 orders/month and 5,000 line items, totaling 5,500 procurement-related records per month. If you take this a step further, procurement transactions such as bulk purchases often involve multiple suppliers. Generally, 15% of purchase orders (75 orders using the previous example) have multiple suppliers, with an average of 3 per order, adding 225 supplier records to the total above. When you consider purchase orders, line items, and suppliers - that is 5,725 rows of data each month and over 68,700 rows of data per year for a company with only 500 employees.

Given the scale of data involved for most organizations, efficiency and effectiveness are critical. You can imagine the nightmare if you had to perform these steps manually or if you made a mistake early on that meant you had to redo everything. Without an automated, organized flow of sufficiently modularized data, it would be incredibly inefficient if an error is later found in your manual process.

Data collection can be automated with the help of SAP experts and ABAP programmers. When preparing this type of solution, it is essential to keep in mind that tables might change, so you will want the flexibility to add custom fields as well as filters to exclude data that is not required (e.g., a specific entity, vendor or customer type).

Vendors like Case IQ have built ABAP integrations to support their suite of compliance software, so companies do not need to invest in additional tooling or develop in-house custom programs. By leveraging existing solutions, companies can bypass the need for hiring a dedicated development team and divert those resources to other core business areas. This not only saves costs but also allows for faster deployment of your compliance analytics solution. Off-the-shelf tools also provide a comprehensive and cost-effective solution for data management, offering benefits such as reduced development and maintenance costs, faster deployment, access to innovation, better support, improved security and compliance, and scalability.

3. Risk Ranking/Scoring and Analysis

Methodology:

Risk Ranking (also known as “Risk Scoring”) is industry best practice to allow companies to prioritize the highest-risk transactions for review. Risk Ranking is the process of assigning a numerical score to a transaction based on the level of risk it poses to the organization. The score prioritizes which transactions or activities compliance teams should review or investigate further.

To give a simple example, imagine a company receiving an average sized invoice from a vendor. That invoice, nonetheless, might have a high-risk score because it was anomalous compared to the usual amount paid to that vendor, was paid without a corresponding purchase order and was paid on an expedited basis (e.g., within 2 days of receiving the invoice rather than the typical 60 day vendor payment window). In this case, the Risk Score might be determined by assigning points to those various risk factors, each of which would be weighted in terms of importance. For example, each of those factors would add points to the Risk Score but the fact that the payment was expedited might add more points than paying an anomalous invoice amount for that specific vendor. Transactions with higher scores would be flagged for further review, while those with lower scores would be given less attention or not reviewed.

As mentioned above, it is imperative to risk score the overall transaction only once, combining the PR, PO, Invoice, and Payment data into one transaction score. More basic approaches that risk score each item separately likely will miss key risk indicators, while also multiplying the number of transactions to review.

Risk Scoring typically requires a methodology or formula to aggregate all the analysis results. There are various ways to do this; however, two fundamental components to consider are the volume of Risk Results in the transaction as a whole (the more results, the greater the risk) and the value of any particular Risk Result (which is based on the severity and the importance of each Risk Result).

For both volume and value considerations, you need to consider the variety of your analyses and ask yourself whether the Risk Result detects targeted or primary risks or secondary risks. For example, a primary risk indicator might be a Risk Result that shows that the vendor matches a vendor listed on the OFAC watchlist. In this case, the value of that Risk Result should be very high, as this transaction should move to the top of your priority list. Similarly, payments to vendors in cash might also have a high value (though potentially lower than an OFAC match).

Other Risk Results may detect secondary risk (e.g., a vendor is based in a high-risk country, the transaction value was a round number). Generally, Risk Scoring can be complicated, but if you lay out a methodology to consider these items by themselves and in relation to one another, you'll begin to see how your work will help prioritize your transactions for review.

Baselining and Refinement:

Now that the complex piece is out of the way, it's crucial to analyze your ERP data for at least 12 months to have a proper risk baseline and establish appropriate thresholds. You will likely refine your settings multiple times during a pilot/sandbox period and re-score to strike the right balance between high-risk transactions and your optimal volume of transactions to review. Once that work is done, you would be ready to start monitoring your transactions in real time going forward.

You should note, however, that you will need to continually refine your analytics as you learn over time, identify new risks and see new patterns of non-compliance within your company or across your industry. You should ensure that you understand how, and by whom, your analytics will be updated, as the ongoing maintenance of, and resourcing for, such systems is often under-estimated. Off-the-shelf products, such as Case IQ's Compliance Monitoring software provide prebuilt analyses that can be modified through a no-code user interface, so that you do not need any data science, data engineering or programming/SQL expertise to modify analyses and maintain analyses over time.

Transaction Analysis:

Once a transactions is flagged for prioritized review, the following steps can help to adequately determine whether the transaction raises true risks of non- compliance:

- Gather the full context of the transaction and related subject (e.g., vendor or customer)
- Understand the underlying details of the transaction
- Explore the transaction in its native system (e.g., SAP) if required
- Explore the subject as a whole (i.e., are there other transactions noted for the subject? What are the company's overall spend habits with the subject?)
- Understand each of the Risk Results produced by the compliance analytics platform and how they relate to one another
- Pair the transaction / subject context with the reason for the Risk Score (i.e., why was the transaction noted as high risk?)
- Quickly move on from transactions that are not worthy of further review, by recognizing false positives as well as known items (e.g., the issue is already part of another review process or has already been assessed not to raise a risk)
- Follow-up on transactions that have a basis for additional review, including by reviewing contracts, speaking to the individuals involved and reviewing email correspondence
- Provide feedback on the transaction and underlying analyses to improve your analytics settings and, ideally, feed a supervised machine learning model to improve the accuracy of your risk analyses over time

4. Root Cause Analysis and Remediation Tracking

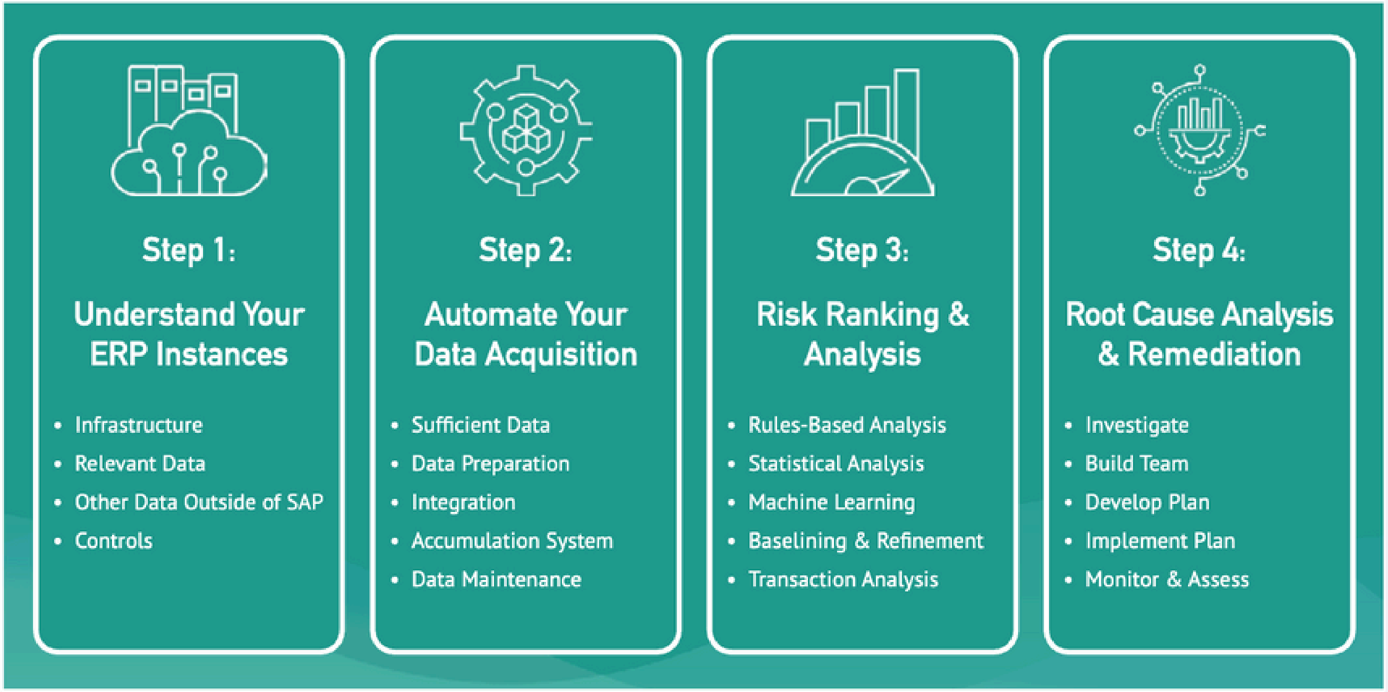
Conducting a root cause analysis of compliance issues and implementing remediation for misconduct is an important process to help prevent future incidents and ensure compliance with applicable laws and regulations. According to the criteria for Evaluation of Corporate Compliance programs from the U.S. Department of Justice, “Prosecutors should also consider whether the company undertook an adequate and honest root cause analysis to understand both what contributed to the misconduct and the degree of remediation needed to prevent similar events in the future.”

Here are some steps to guide you through the process:

- Identify the compliance issue: Start by identifying the specific compliance issue that occurred. Determine the nature of the misconduct, who was involved, and when it happened.
- Assemble a team: Bring together a cross- functional team with expertise in the area where you had the compliance issue. This team may include representatives from legal, compliance, audit, finance, human resources, and other relevant departments
- Conduct a root cause analysis: Use a structured approach to identify the compliance issue’s root cause(s). The process may include conducting interviews with employees involved, reviewing relevant documentation, and analyzing processes and procedures to determine what caused the failure (e.g., willful non-compliance, human error, control gap, lack of training, etc.)
- Develop and document a remediation plan: Once the root cause(s) have been identified, develop a plan to address the issue(s) and prevent it from happening again. The plan should include specific action items with timelines and responsibilities assigned to individuals and should be documented.

- Implement and track the remediation plan: Put the remediation plan into action. This may involve updating policies and procedures, providing additional training to employees, or making changes to the company's culture or governance structure. The remediation plan's implementation should be tracked through to completion with a full audit trail.
- Monitor and assess effectiveness: Continuously monitor the implementation of the remediation plan and evaluate its effectiveness. This may involve conducting audits or risk assessments to ensure the compliance issue has been adequately addressed and prevented from reoccurring.
- Communicate with stakeholders: Keep stakeholders informed throughout the process, including employees, customers, shareholders, the Board and regulators. Transparency is key to building trust and credibility.

Remember, conducting a root cause analysis and implementing remediation is an ongoing process. Every incident or problem provides an opportunity to improve your systems, procedures, training and/or processes. Conducting root cause analysis helps in identifying the underlying cause of the issue, and implementing remediation helps prevent the problem from recurring. By regularly conducting such analyses, an organization can identify areas for improvement and continuously improve its compliance program. All root causes analyses and any related remediation work should also be clearly documented with an audit trail, ideally within your compliance analytics platform itself.



Step 1:

Understand Your ERP Instances

- Infrastructure
- Relevant Data
- Other Data Outside of SAP
- Controls

Step 2:

Automate Your Data Acquisition

- Sufficient Data
- Data Preparation
- Integration
- Accumulation System
- Data Maintenance

Step 3:

Risk Ranking & Analysis

- Rules-Based Analysis
- Statistical Analysis
- Machine Learning
- Baselining & Refinement
- Transaction Analysis

Step 4:

Root Cause Analysis & Remediation

- Investigate
- Build Team
- Develop Plan
- Implement Plan
- Monitor & Assess

Conclusion

Compliance is critical for organizations that want to operate ethically and responsibly. Leveraging SAP data can provide organizations with the robust data needed to mitigate compliance risks and stay ahead of potential issues. By following the four steps outlined in this guide, you can start your journey toward an even more effective compliance program that prevents, detects and remediates compliance risks. Remember, you don’t need to start using all your data simultaneously. Start small and build on your initial successes. By continuously monitoring and assessing the effectiveness of your compliance program, you can identify areas for improvement and continuously improve your systems, processes, controls and training. In conclusion, take advantage of the comprehensive and structured information in your SAP ERP to identify patterns, detect risks, and empower your compliance program using data analytics. Use the steps outlined in this guide to stay compliant with regulations, prevent critical problems, and ensure your organization operates ethically and responsibly.

One-on-One Advice

Our team of experts has implemented Case IQ for compliance teams around the world.

They are available - free of charge - to speak with you and share the best practices we've learned. No pushy salespeople, just a chance for you to learn from our experts.

With our suite of compliance tools, reporting hotline, and case management software, plus a 25-year track record of successful implementations, Case IQ is the global leader for end-to-end compliance risk management. To get a demo please visit www.caseiq.com/request-a-demo.

To book your one-on-one, please contact:

☎ (800) 465-6089

✉ sales@caseiq.com
media@caseiq.com
support@caseiq.com

300 March Road
Suite 501 Ottawa,
Ontario K2K 2E2
Canada

DON'T MISS OUT
Visit CaseIQ.com for more great investigation resources.