

5 Steps to Getting Started with Compliance Data Analytics

Contents

5 Steps to Getting Started with Compliance Data Analytics	3
Why Take a Data-Driven Approach?	4
The 5 Steps to Implementing a Successful Compliance Data Analytics System	
• Step 1: Set Your Vision	6
• Step 2: Assess Your Current Strengths and Weaknesses	10
• Step 3: Identify and Use the Data	12
• Step 4: Implement and Refine	16
• Step 5: Embed Data-Driven Risk Management	18
The Next Step	19

5 Steps to Getting Started with Compliance Data Analytics

The 2020 update to the US Department of Justice (DOJ) compliance guidance, Evaluation of Corporate Compliance Programs, has been a wake-up call for many organizations to reevaluate their compliance program and think creatively - and strategically - about its effectiveness. In the intervening period, the DOJ and US Securities and Exchange Commission (SEC) have both signalled a shift towards a more aggressive enforcement of rules that discourage corporate wrongdoing and an expectation that companies will anticipate risks, not simply rely on after-the-fact intelligence from sampling or whistleblowers. And, while the US is taking the lead from a regulatory perspective, existing and strengthened anti-corruption legislation in the UK, EU and beyond means we can expect other governments to soon follow suit.

Data analytics and automation provides a significant opportunity to modernize the mechanisms used to identify compliance risks within businesses, particularly in areas such as fraud, corruption, sanctions and conflicts of interest. By utilizing the data that is already being collected, it's possible to anticipate areas of risk, and identify, in granular detail, insights relating to wrongdoing.

What is Data Analytics?

Data analytics is defined as the science of analyzing raw data to draw conclusions. In this context it means layering and connecting transactional data that exists within your organization and providing meaningful context to identify risk. It is the alchemy of transforming raw data into usable information that can guide action.

This guide will help you to consider the five steps you need to take to leapfrog your existing systems and embrace the advantages of using data analytics to become more efficient and effective in detecting risks and preventing wrongdoing.

Why Take a Data-Driven Approach?

Using the data that you already have within your organization to help you to identify and manage risk has multiple benefits.

It's faster and more cost effective. A data-driven approach that tracks multiple risk metrics will identify corruption and financial crimes more quickly. This is because it makes it easier to join the dots between silos of information to identify anomalies and areas of non-compliance. In its 2020 global study of workplace fraud, the ACFE found that the average fraud case lasted 14 months before detection and that companies lose 5% of their revenue from fraud. This figure alone makes a case for the return on investment of creating a data-driven early warning system.

It meets regulatory requirements. The DOJ has been clear that companies must assess the effectiveness of their compliance programs, focusing on the outcome of these programs, not simply their existence or how detailed they are. A data-driven methodology demonstrates a proactive approach to identifying risk, addressing DOJ concerns. More than that, the DOJ knows what is possible, as they are using data analytics internally and have noted that they have seen first-hand several corporations' best practice efforts using data analytics. If you ever find yourself in front of a regulator, a functioning data analytics program can garner credit from them by showing either that data analytics helped you detect issues quickly or that the behavior was so rogue or anomalous that it evaded your best faith and sophisticated efforts at detection.

Better decision making. Giving different levels of your organization, from middle managers to the C-Suite and board, reliable and consistent risk data makes for better corporate decision making. Putting risk data in the hands of these stakeholders means they can embed risk analysis directly into their commercial and strategic decision making and be held more accountable for the risks raised by those decisions.

Your team profile. When data analytics are used effectively, they give your compliance, legal, internal audit and investigations teams the opportunity to work on higher-value activity. Risk analysis and audits can be run automatically using data and algorithms, identifying priority risk areas on which your teams can focus. This not only increases efficiency and effectiveness, it also builds the internal credibility of your team and gives them the satisfaction of making a greater impact on the business.

Digital transformation has touched so many areas of our lives from how we work, to how we access finance and our health and wellbeing. Using data to transform compliance and risk management is an obvious next step. So if getting left behind isn't an option, where do you begin?

The 5 Steps to Implementing a Successful Compliance Data Analytics System

Step 1: Set Your Vision

Firstly, you should set a vision (and scope) for what you want your data analytics program to achieve. This should be more than simply compliance with regulations: data analytics has already transformed marketing and financial data into a powerhouse for decision making and has the potential to transform your organization's approach to risk, so think big.

“Organizations building or updating their compliance programs, or reassessing their legacy programs, have the opportunity today to leapfrog old approaches and embed new technology-driven strategies that already promise better outcomes and will undoubtedly lead to unexpected benefits down the road.”

-Parth Chanda, CEP Magazine, May 2021

At this point, you are making the case within your organization for what could be a significant change. You will not only need access to existing data and systems from across your organization today, but - ideally - be involved in the future development of new systems so that new data sources can be incorporated into your risk management data system.

Organizational resistance

There may be some internal resistance to the idea of integrating data within your organization, so consider the approach and communication plan up front. The board or C- Suite might be right behind you, but you may need to consider how else you can gain support across the organization and utilize other internal and external networks. A C-suite champion for your project and a plan for communicating the need to change across your organization will make a significant difference to the level of cooperation you receive from key internal stakeholders.

For some organizations - and compliance teams - there is a fear that using data analytics to tease out risk will open a Pandora's box of problems. One common objection is that the impact on the internal audit or compliance team will be overwhelming or it will uncover hidden risks, such as widespread fraud or corruption, with resulting negative PR consequences.

The reality is that it is better to uncover problems and manage them proactively than wait for a whistleblower, a regulatory investigation, a costly legal case and/or a PR disaster. If this is a barrier to change within your organization, address it upfront. The DOJ (and its leading international counterparts) is likely to take their 20/20 hindsight once they become aware of an issue to call into question the company's failure to detect issues earlier.

Start with the end in mind

The purpose of setting a vision is to have a clear end point that you can use as a 'north star' to navigate throughout the project.

“One of the main pitfalls when starting out is not identifying the main goal. Teams jump to the tactical elements, like visualizing data, and forget about the strategic goal which might be introducing transaction management for risk.”

-Parth Chanda

Although the eye-catching tactical outputs can sell a project, clarity about the main objective provides a laser focus as you progress. For example, a data visualization of your vendors by spend amounts may not be as helpful as risk scoring your vendor spend items to identify true risk in your data. Defining the end point at the start and then keeping it front and center throughout the project will ensure you aren't sidetracked by internal wrangling or blinded by technical jargon from the IT department.

Plan for the user experience

Another element to consider is the end-to-end user experience of your eventual system solution. Although you may be using existing data sources, it's worth considering who is inputting that data (potentially your entire workforce) and any changes that would need to be made to ensure the consistency and integrity of the data, no matter who enters it. An example might be organizations with decentralized expenses systems - the data needs to be comparable across these decentralized units, potentially changing the user experience at point of entry.

At the other end of the process, you need to think about who else will use the final information and how easy it will be to access and run reports. For example, will you need to segregate access to the data so that territories can only access their own data? All these elements will define the final user experience and should be part of your vision. In other words, start with your final outcome clearly defined and be clear about the 'why'.

Actions

This vision setting stage should identify:

- The primary goal or output that you are seeking to achieve
- Any secondary objectives. These might include broader digital transformation, the impact on your team, regulatory compliance, better decision-making data etc.
- The scope and scale of change required in the culture and systems to make this a reality, including any organizational resistance
- The stakeholders needed within your organization to champion the scale of this change.

Step 1: Assess Your Current Strengths and Weaknesses

If step one is making a clear, coherent case for where you want to be, then step two is a clear, coherent examination of the current situation.

Identify weaknesses and/or barriers

You will first need to assess your existing compliance program and its use of data. There will definitely be strengths in your current practice, but also weaknesses, which may include:

- A lack of real-time data analytics, reporting or monitoring
 - Result = missed anomalies and patterns of risk
- Too few legal or compliance resources to support the business
 - Result = insufficient targeted action, reactive, non-compliant with regulatory requirements
- Disorganized, disparate, multiple, localized and/or disconnected data stores and/or data entry
 - Result = compliance leaders feeling increasingly overwhelmed with the disjointed information that's available, missed anomalies and patterns of risk

These weaknesses can create a reactive culture, one that makes subjective judgements on where to focus attention and resources which will, in turn, determine what is eventually found. This is exactly the pattern of practice that the DOJ is seeking to change.

In step one you may have identified these as drivers for change but step two is a more forensic examination of the realities of your compliance program. An ambitious vision that is tempered by a reality check, grounded in practicalities, will improve the chances of a successful realization of that vision.

Define an action plan

With a clear view of what you want to achieve through a data analytics program and the strengths and weaknesses of your current system, you can define an action plan.

Trying to do everything at once is a common pitfall. If you are overwhelmed by the sheer amount of change required, identify the best place to start by taking a risk-based approach - where is your organization most vulnerable? This may emerge from pain points or from previous incident reporting. Focus on those areas where you'll make the biggest impact so that your action plan is achievable and then take a phased approach to everything else. Your action plan should set out roles and responsibilities, timing and resources required.

Resourcing the plan

Whether you already have a large in-house IT team of data scientists or are looking to create a team, there is a significant difference in the resources required if you build your own data analytics system compared to buying one off-the-shelf.

The decision to buy or build may be predetermined due to the complexity of your systems or internal politics. Building in-house can be fraught with complexity and have significant cost and headcount overheads and the risk that key team resources may move on to other opportunities internally or to another company and stall your efforts. Off the shelf systems can be implemented quickly, more cost effectively and are built around best practice requirements.

A bought system has the added advantage of keeping the project within the remit of the Compliance Team, rather than it spiraling into an 'IT project' that may not be prioritized in the same way.

If you do decide to build a data analytics system in house, having this action plan will be vital in allocating resources effectively so that you focus investment on the vision and opportunity, rather than being side-tracked by existing systems or short term priorities driven by internal politics.

Actions

This assessment should identify:

- The weaknesses in your current systems that might hinder change or shape the priorities
- An action plan with broad timings and responsibilities
- The resources you will need in terms of people, expertise and budget
- Whether you will buy or build the data analytics system.

Step 3: Identify and Use the Data

This is the practical step of starting to identify and use the data that is in your business. The complexity of this stage depends on the complexity and location of the data and the systems used by your company.

Identifying data

In this deep dive phase, the first challenge can be identifying all relevant data sources, especially if they are siloed across departments and/or locations. Your organization may have a patchwork of enterprise systems, SaaS solutions, spreadsheets and databases held centrally or locally.

A good place to start can be by identifying the relevant business processes and systems and then examining the data in each of these, including expenses, invoices, distributor and customer revenue transactions, and third party compliance.

For example:

- Vendor payments from the enterprise resource management system
- Travel and entertainment expenses, including high risk reimbursements for government official expenses
- Distributor or reseller rebates, discounts, free goods and other revenue transactions

This data is proximate to key risks and is also usually well structured with robust export and reporting functionality through finance, HR or ERP systems.

“Data can be overwhelming. Start small and identify data sources that are easily accessible and easily understood.”

-Kara Bonitatibus, CEP Magazine, May 2021

Connecting data

You will also need a tool that allows you to connect and layer the data in an automated way, commonly referred to as extract, transform and load (“ETL”), to transform and harmonize raw data to then be able to derive meaningful information that you can act upon. Ideally the tool needs to pull in data from different sources, risk rate individual transactions and visualize insights. You can build a tool or implement an established tool to facilitate this - the important thing is the quality of insight from integrating data from disparate sources.

The complexity of this stage will depend on the way that your data sources output data, whether that’s through in-house data feeds or external APIs. You will need data engineering resources experienced in data integration to build the system, or source an existing tool that is designed for this purpose. Those data engineering resources will need significant input from data science resources and forensic audit and compliance experts to ensure they are pulling all relevant data attributes needed for your compliance analytics.

Analyzing data

Once data acquisition is automated, you will need to create the risk algorithms that will be applied to your data to derive risk insights. An internal company effort will require a combination of strong data science expertise as well as forensic audit and compliance experts who can educate the data scientists on the relevant fraud and corruption patterns, schemes and risk indicators. Ideally, your risk algorithm will produce aggregated risk scores for transactions, vendors, customers and employees, which will enable you to identify the highest risk issues easily. An established tool with pre-built and configurable algorithms can significantly accelerate your implementation and time to value and reduce the need to hire expensive data science resources. It also can help ensure that your algorithm can be controlled by non-technical users without the need for constant intervention by IT.

Actioning data

A workflow or case management element for your output is also essential to documenting the follow-up and remediation that was taken on the risks identified from your data analytics effort, both to improve your risk model over time and to document internally (and potentially for a regulator down the road) your good faith efforts.

For example, if your analytics identify a high risk vendor payment, your compliance or audit team should be able to easily document the steps they took to resolve the risk flag (e.g., reviewing contracts or invoice documents), their resolution or final judgment (e.g., an issue was identified or not), and any corrective action plans (e.g., a new control, policy enhancement, discipline). The follow-up should ideally feed back into your risk analyses using machine learning to improve your predictive model over time. Internal builds can often overlook this critical workflow need or build this follow-up in a disconnected database or spreadsheet, where its value is severely limited.

Visualizing data

Visualized data has more impact, enabling you to engage your management, C-Suite and board with evidence-based insight that clearly identifies patterns of risk. A picture can be worth a thousand words.

However, the skill is in creating the visualization that helps you to identify risk and make decisions. Great visualizations filter out the noise and provide clarity. For example, a visualization of vendor spend or distributor rebates in a country that also layers on risk scores for those vendors or distributors can escalate a third party that may be average or low in terms of financial value but extremely high risk in terms of the risk algorithm - helping you better identify the proverbial needles in the haystack in large data sets.

The proactive approach set out by the DOJ, emphasizes action, not simply data collection or the deployment of complex systems. Without the ability to contextualize data and visualize it to inform action, your data analytics system still won't meet the expectation of regulators.

Actions

This stage focuses on the practicalities of identifying, connecting and making connections between data sources:

- Identify data sources and the method to access these
- Connect data using a tool that pattern matches and outputs the data in a way that provides context
- Build a workflow and document management functionality to capture follow-up and remediation from your analytics efforts
- Define visualizations needed that relate back to your original objective and provide clarity

Step 4: Implement and Refine

Your data analytics system won't be perfect the first time. Before your system goes live: test, test and test it again. And once your data analytics system is rolling, it's absolutely vital to keep learning and refining the system so that it fits your business, the risks it faces, its needs and the wider context of evolving compliance regulations.

Sense check all the initial findings. Where are the anomalies? It could be that the wrong data is being pulled out of one system or there are problems with making comparisons. It might highlight ways in which data is being collected differently in different locations. Or maybe you have identified risks that you hadn't expected and can immediately act upon.

Refine data sources until you are confident in the insights provided. This is critical for the long-term credibility of your compliance team.

You will most likely need to identify false positives and conduct sensitivity testing to ensure the parameters you are using are configured to uncover the right level of risk. Failure to do this early on could result in you or your team being overwhelmed.

Play with visualizing data until you've captured the key information to report on to your board in a format that they can engage with easily and intuitively. Start small, and build out.

Refine to reflect wider changes. Over time, the context of your business will change, as will the data that is available. The organization may change its expenses policies for example, or move into a new territory, change its ERP system, etc. Your data analytics system must evolve to reflect this, making it a dynamic tool that is integral to risk management within your business.

The DOJ guidance explicitly calls on prosecutors to examine whether an organization's "risk assessment is current and subject to periodic review". Building an analytics system, without considering how to update it, risks failing to comply with regulations further down the line.

A common pitfall is to underestimate how resource-intensive, and yet how vitally important this stage is. If you've built a system, you will need to maintain it, refining it to reflect changes in data sources, internal policy or government guidance. If you have built your system rather than sourced a pre-existing solution, this means having data engineers, data scientists and forensic experts on hand to make changes. If you have recruited for these roles, then consider retention and/or succession planning - a highly bespoke system that relies on an individual or small team is vulnerable.

Actions

This stage is all about ongoing maintenance and continuous improvement:

- Keep refining your system so that it meets those primary and secondary objectives identified at stage one
- Monitor changes to internal systems, data sources and policies so that the data that feeds your analytics system continues to have integrity
- More broadly, ensure you have the resources to keep the system kept up to date -whether that is through a SaaS solution or access to internal data engineering, data science and forensic audit/compliance resources

Step 5: Embed Data-Driven Risk Management

Data analytics is not an end in itself - it is the means to an end.

The end point of a data-driven approach to risk management is to provide a catalyst for change: to be proactive and objective in identifying and reducing compliance risk. Tick-box compliance is not good enough, as regulators increasingly expect organizations to prove the effectiveness of their programs. Data provides the evidence needed to do just that.

If in stage one, there was organizational fear of opening a Pandora's box of problems, at this stage those fears may be realized. But equally this is where those problems can be identified and tackled, efficiencies can be gained and a return on investment begins to emerge.

Having the relevant data insights at your fingertips and refining your systems can prompt broader changes, especially if you learn from that data over time. Maybe you are able to shift the responsibility for some areas of compliance to other parts of your organization on a functional or geographic basis? Better data allows you to take a risk-based approach to compliance which can mean dialing down processes in some areas, while dialing it up in others.

Actions

This is the stage for organizational action:

- Engage your board and C-suite to address systemic issues identified by the data
- Flex compliance systems depending on the patterns of risk identified and the culture within your organization

The Next Step

For most organizations, connecting data sources, analyzing data and visualizing patterns can be a significant step forward. Whether you buy or build a system, it's inadvisable to shortcut these five stages - they should be considered foundational.

However, once you do have a robust set of data analytics, there are groundbreaking opportunities offered by automation, machine learning and AI. Platforms like Case IQ have integrated AI and machine learning so that the refinement stage is continual and ongoing. The system learns from your data and provides predictive insights into risk.

Unfortunately, it's impossible to leapfrog to predictive insight without the foundational efforts of implementing a robust data analytics system. But working with an experienced, specialist company will shortcut the pain and cost of an in-house development.

Buy or build, data-driven risk management through data analytics is good for business: ethically, legally and financially. The DOJ guidance might be a call to action, but the opportunities to transform risk management within your organization are so much greater than just regulatory compliance.

Good luck on the journey!


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.