Case IQ

EXPERT GUIDE

Making the Business Case for Compliance Monitoring Using Data Analytics

Featuring Hui Chen, former Senior Advisor at Ropes & Gray Insights Lab and Compliance Counsel Expert at the U.S. Department of Justice (2015-2027), Justin Ross, former Vice President and Global Chief Compliance Officer at FedEx, and Parth Chanda, Founder of Lextegrity, EVP, Risk and Compliance Transformation at Case IQ.

Hui Chen

Hui is a former Senior Advisor within R&G Insights Lab and an international leader and expert in organizational integrity. She was the first Compliance Expert at the U.S. Department of Justice and authored the “Evaluation of Corporate Compliance Programs” document that redefined compliance expectations. She began her career as a federal prosecutor in the Department of Justice in Washington, D.C., and the Eastern District of New York. Hui has extensive in-house experience as a senior legal and compliance leader at Microsoft Corporation, Pfizer Inc., and Standard Chartered Bank in locations across the globe, including Munich, New York, Beijing, and London. Hui is a thought leader who has published frequently in legal, business, and academic journals, including the Harvard Business Review. At the R&G Insights Lab, she advised clients on a broad range of strategic issues and continues her thought leadership with publications, webinars, and podcasts.

Justin Ross

Justin served as the Vice President and Global Chief Compliance Officer for FedEx Corporation from 2019 to 2024. He led the team responsible for FedEx’s enterprise compliance programs, including anti-corruption, antitrust/competition law, data privacy, trade/export controls, and hotline management and investigations.

Throughout his career, he has held various roles in the FedEx Legal Department both in the United States and internationally. He now serves as the Vice President and Chief Compliance Officer at Sysco.

Parth Chanda

Over the past 20 years, Parth has established himself as a leader in the field of compliance, and served as the Founder of Lextegrity until its acquisition by Case IQ, where he currently serves as EVP, Risk and Compliance Transformation.

Case IQ’s* software has been before regulators on several occasions and was recognized by the SEC as a remediation factor in a client’s FCPA resolution in 2020. Prior to Lextegrity, Parth served in various global compliance roles at Pfizer, where he oversaw multi-year transformations of its global compliance program, including re-drafting policies and procedures, implementing new third-party due diligence processes, enhancing integrated internal and financial systems and controls, and guiding cross-functional risk assessment and data analytics initiatives. Prior to Pfizer, Parth was hired to oversee the enhancement of Avon’s global anti-corruption compliance program after its voluntary disclosure of FCPA matters to U.S. authorities. Parth began his career at the law firm of Shearman & Sterling, where he was the Contributing Editor of its FCPA Digest.

*Lextegrity was acquired by Case IQ in 2025 and is now oered as an end-to-end suite of compliance tools.

In today's increasingly complex business and regulatory environment, ensuring your compliance program is truly effective is critical but highly challenging. Technology, if deployed correctly, can play a significant role in preventing and detecting non-compliance and helping an organization objectively measure the effectiveness of its program. However, making the business case for such technology investments to upper management and the Board is often a challenge for in-house compliance professionals.

In this Expert Q&A, three compliance practitioners with deep experience within corporations, the government, and technology share their insights on how technology can help ensure your compliance program is effective and how you can make the business case within a company for such technology.

Hui, you have thought about compliance program effectiveness for many years from the perspective of in-house, government, and now advisory work. Let's start with the existential question at the heart of this Q&A: "What is an effective compliance program?"

HUI CHEN: An effective compliance program is a program that does what it sets out to do, which for a compliance program is to prevent, detect, and remediate violations of laws and policies. So that's the short definition.

When an organization or person is effective at something, that means that they're accomplishing what they set out to do. So, these are efforts that you make, for example, in the areas of training, communications, educating your employees, and guiding their conduct so that they can stay on the right path. To put it in an analogy, at a crossroads, you put up all manner of signs so that people do not go down the wrong path. That's prevention. Detection is for when people go down the wrong path, and you know that your first line has failed. They did go down the wrong path, either intentionally or by mistake. Then the question becomes, how quickly can you catch it? So, it's a question of whether they go 10 yards down that path, and you can stop them and say, whoa, not this path - go back, go back. Or do they go 10 miles, 20 miles, or a hundred miles on that wrong path, and you don't even know?

So, detection is about your ability to find out what has gone wrong, and one of the important ways of measuring that is how early you can detect it. When you find wrongdoing, and by the time you find it, it has been going on for ten years, that's a much bigger problem. That is a bigger failure than if you have found something just hours or days into it.

Finally, when you find a mistake early and quickly, remediating the mistake is much simpler. So, after somebody has done the wrong thing, how do you fix the system so that any damage caused has been repaired? And do you do everything possible to ensure the same thing does not happen again?

Parth, as a former in-house compliance lawyer who now builds compliance technology, how is technology evolving to support Hui's vision of an effective compliance program?

PARTH CHANDA: There is an adage that your compliance program should never be a "check the box" program. What that means to me is that your program should not be superficial window dressing. Instead, it should actually prevent wrongdoing and, when wrongdoing undoubtedly occurs, should detect it as close to immediately as possible, as Hui has so eloquently laid out with her crossroads analogy. The traditional compliance technology suite has included approval tools for things like gifts, donations, and third-party due diligence, a training platform, a hotline, and maybe a data visualization tool to visualize the metrics generated by those tools, such as your training completion stats and the number of high-risk third parties by country from your diligence program.

These tools continue to form the foundation of any good compliance program, but there is now a recognition that they are necessary but insufficient at objectively measuring whether your program is actually effective. For example, hotline reports that are substantiated or negative audit findings may provide clear evidence that the compliance program is not working on the ground, but the lack of such findings cannot be relied on to tell you that your program is effective. The lack of reporting and substantiation may arise instead from a fear of reporting, the deliberate hiding of wrongdoing from investigators, or their inability to access key documents and communications. Similarly, audit findings are based only on a sample of countries selected and a sample of transactions selected in those countries, and those selections themselves may be informed by where the company believes they have risk rather than where they actually have risk, missing whole swathes of risky behavior.

Other compliance metrics often only show that processes are working and not necessarily that wrongdoing is not occurring. Training completion rates, code certifications, and approval and diligence process statistics only show that employees or third parties are completing process steps that they start, not that they are initiating them in all required cases or being truthful when they complete them.

Increasingly, companies are turning to the use of real-time data analytics technology to test all transactions as a better approach to testing for non-compliance in real-time. Such technology can apply advanced behavioral, statistical, and policy-based key risk indicators to each transaction flowing through an organization's systems, such as payments through financial systems, to score each transaction and find hidden compliance risks in large data sets. Running tools like that allows compliance officers to detect when someone has gone down the wrong path for 20 feet in Hui's analogy rather than 20 miles and to remediate those issues closer to real-time before the issue becomes systemic. I think these types of tools will become table stakes for compliance professionals in the next three to five years.

Justin, as the leader of the compliance program at a Fortune 50 company with over 500,000 employees globally, how did you articulate what technological changes you wanted to make to your compliance program to achieve what Hui and Parth have laid out?

JUSTIN ROSS: For me, coming up with our priorities for improving our compliance program is a combination of understanding our key regulatory requirements and overlaying that with our traditional risk assessment process. At this point in time, some of our key regulatory requirements revolve around export controls and sanctions and other third-party risks and the heightened expectations of real-time transaction monitoring. So, we approached our risk assessment with those requirements in mind to assess where our biggest risks lie. At the end of that process, we knew that we needed to prioritize more advanced transactional monitoring using data analytics on our third-party payment data.

Simultaneously, you might also get feedback from your Audit Committee or broader Board that we should be looking into certain areas. You love to hear that when you are looking for resources, and those items then jump to the top of my list. And this was a case where the Board's priorities lined up exactly with our priorities coming out of our own risk assessment to drive us to implement more advanced data analytics and monitoring capabilities.

Once we knew the goal, we then had to engage with the relevant data owners to make the goal a reality, so we engaged with IT and Finance, who are more intimately involved in the financial data needed for transactional monitoring. It is important to build a cross-functional team that involves the relevant data owners and experts and make sure they are aligned on your overarching goals for your technology enhancements.

As a follow-up, there's a lot of discussion on how to show a return on investment, or ROI, for investments in compliance monitoring using data analytics. How did you think about ROI and position the ROI internally to your management and Board?

JUSTIN ROSS: Building the ROI rationale definitely depends on the project and its goals. In this space, you can definitely show ROI for fraud prevention and detection. At FedEx, like most organizations, we have external fraud and internal fraud. External fraud is mainly customer-related fraud due to fraudsters inappropriately accessing customer accounts, and internal fraud is related to employee misconduct, such as embezzlement and asset misappropriation. So, we track the total cost of fraud to help build the rationale for specific tools to help us with fraud detection and prevention.

In the external fraud space, we have shown how these tools can help reduce fraud over time and create significant cost savings for the company. We have been able to show that the total cost of fraud this month was here, and the total cost of fraud went down. This type of data has helped us build the ROI case for tools looking at internal fraud.

But the other ROI factor that should not be overlooked is back to the expectation of enforcement agencies and regulators. For transaction monitoring in particular, enforcement agencies such as the SEC and DOJ now expect that, so the company has to do something in this space. That has been a powerful and successful argument for building a compliance analytics program focused on detection.

Finally, we expect our investments in compliance data analytics also to help the business be more efficient and operate faster. One example of this has been in the third-party vendor risk management space. Sometimes the business says we are too slow with vetting our vendors. So, if we can get tools to make that faster and more efficient, that's where you can really help the business. We can say, "We can make this faster, but we need this investment and this technology to do that."

HUI CHEN: To add to Justin's comments, you should continue to build your business case as you implement such tools. First and foremost, you should be taking a baseline measurement before you implement anything or just as you start to implement something, and then take those measurements at regular intervals, such as six months or 12 months. This will help you capture many of those wins and move them beyond the individual anecdotal stories to much more holistic data-driven narratives. So, where you can go from, "We detected this individual payment or made sure there were no duplicate payments," to telling your management or Board, "When we started this program, we were paying X million in duplicate payments, and six months later it was reduced by 40% and twelve months later it has been reduced by 80%." That is a much more compelling and powerful story, but one you can only tell if you have taken that baseline.

Some of the challenges of building a business case are to identify the appropriate size and scope of your compliance data analytics project. How have you done this?

JUSTIN ROSS: A helpful strategy for our team has been phasing and scaling. And what I mean by that is start small and grow in phases from there. So for instance, FedEx operates in 220 countries with over 550,000 employees. If we jump into a transaction monitoring project for the whole enterprise, that is an enormous amount of data and output to manage, as well as a large spend outlay. But if we start in phases, with a handful of countries, for example, we leverage a smaller amount of data at a lower initial cost. We can then test it out and see how it works. And then, if you have some successes out of that, you have some data that you can show your executive leadership team and Board of what you found at a small scale, which is an excellent advertisement for the expansion of your program.

This is exactly what we have done with vendor payment transaction monitoring. We're starting small with specific countries and certain amounts of data. We're showing what we can do with that and some successes with that, and then we will advertise that to executive management and the board to get more support for enterprise-wide rollout. That also allows you to be agile - to start small, and if the first phase of your project fails, and I've had those as well, you can stop quickly and pivot to something else without having wasted too much time or money.

PARTH CHANDA: Back in 2015, when I was in-house at a large global pharmaceutical company with over 100,000 employees, I had to convince the Chief Compliance Officer that transactional-level monitoring was the next generation of third-party risk management. I did exactly what Justin described by selling him on an initial phase that involved a small geographical universe while making sure that my counterpart in Audit had a seat at the table to leverage the output of the data analytics. Once that first phase was completed successfully and both functions had seen clear benefits, the company then embarked on a global implementation over successive phases. But the project literally began with one idea and two people in a room, discussing a highly feasible first phase that did not need Board or executive leadership team review and approval. But when the successes flowed from the first phase, and we began contemplating a global roll-out, we had a slew of excited stakeholders from audit, finance, procurement, and compliance bought in and ready to expand the program.

Fortunately, compliance data analytics and monitoring technology are far more accessible from a cost and effort perspective today than it was in 2015, so depending on the size of your organization and your budget, you may be able to do a global implementation or phase-in analytics over a smaller number of phases. But it is critical to identify the risk domains (e.g., vendor spend, customer and distributor revenue, travel and expense, etc.) and geographies or businesses you are most focused on from a risk perspective to create the optimal phasing plan.

HUI CHEN: You can also start by studying the data you already have. Before you get to anything fancy at all, use the traditional data that you have to understand the problem. What do problematic transactions look like? What are their attributes? Then take baby steps, which I strongly and consistently advocate because not only is it cheaper, but it also has many other advantages. It's more manageable when you do a couple of smaller phases with a couple of specified business units instead of the entire company. It also gives you more data to study to see how it works, what changed, what got better, and what needs to be tweaked. You're using a scientific, experimental mindset. You're studying what you have and taking baby steps to test something and use what you learned to gradually expand your program. Those approaches are crucial to anybody wanting to make significant organizational changes because, when you start with those baby steps, you have a lot more evidence and data along the way to convince your stakeholders, as well as just being able to manage the projects a lot more efficiently.

Did you ever consider building your compliance data analytics and monitoring internally? What are some considerations?

JUSTIN ROSS: I would be very careful about building your own compliance tools internally or listening to an internal group that says they can do it for you. FedEx has the best IT team in the world, but they are pulled in 20 million different directions. We have had experiences where IT has built a compliance tool for us, but over time, they haven't been able to maintain it or get the budget to keep the people to support it. There are all kinds of internal issues we have run into there. So that's been a challenge that we have learned from.

I always will lean towards a vendor first because the vendors are experts in their field. FedEx, we deliver packages, not compliance tools. I would be careful about listening to internal folks saying they can build your compliance data analytics and monitoring tool.

PARTH CHANDA: When you go beyond data visualization to true aggregated forensic data analytics on financial data to look for compliance risks, you are talking about an order of magnitude of complexity. There is often an underestimation of the human and technological resources needed to stand up and maintain a system like that. The people resources run the gamut of data engineers, data scientists, database architects, forensic accountants, application developers, and data visualization experts to create the database, analytics engine, workflow engine, and visualizations for you. As Justin mentioned, you will also need to maintain all of these people over time to support the program. Beyond that, a number of different external software tools will need to be licensed across all of these realms to stand up your internal program.

But ultimately, even if you have those resources, will you be building a best-in-class solution that leverages learnings and feedback from multiple companies? A vendor that is competing in the marketplace in the specific compliance monitoring and data analytics space will likely have a much stronger offering than one you can develop and maintain internally and one that will likely cost you less all-in when you take into account the human resource and software costs you will need to incur to build and maintain an internal system.

Though the Department of Justice expects companies to leverage their data in their compliance programs, companies remain hesitant about investing in compliance data analytics. Hui, can you provide your last word in terms of how you try to convince companies to take the plunge?

HUI CHEN: Using data in compliance is about more than just satisfying the prosecutors if and when you get in trouble. It is about compliance demonstrating value to the rest of the company every single day. Yes, using data analytics is in line with Department of Justice expectations and can help companies avoid expensive and reputation-damaging legal cases. More importantly, compliance teams that make use of business data can uncover everything from fraud to waste and inefficiencies in the company's use of resources.

When compliance data analytics identifies issues such as duplicate vendors or invoices or paying vendors too quickly, compliance can literally quantify its contribution to the company's bottom line. Once compliance data analytics are implemented, functions beyond Compliance across the enterprise can benefit. Internal Audit teams can reorganize their efforts to focus less on labor and cost-intensive periodic sample-based audits, where they fly a team of auditors across the world for two weeks to review a small sample of transactions, to leverage more comprehensive data analytics and do deeper forensic reviews and third-party audits based on the findings of the data analytics. The Investigations team can access real-time data – risk-scored transactions for vendors and employees – without having to reach out to IT and Finance, and can then scope and resolve their investigations far more quickly and satisfy the ever-present demands of the business leadership for faster close-out of investigations. The Finance and Procurement organization can use the same data analytics to review existing and new third-party engagements and rationalize the vendor base to reduce risk for the organization.

And finally, business leadership can have objective data showing their spending and risk and feel more empowered to decide whether the money they are spending is justified by the risk posed. Compliance teams often talk about shifting accountability for compliance to the business - for them to "own their compliance." What better way to do that than to give the business the tools to do just that - actual risk data for their teams' financial transactions?

The Problem We're Solving

We focused on the challenges every compliance team faces:

- Employees lacking sufficient tools to assess risk and own their own compliance
- Too few legal or compliance resources to support the business
- Risks managed in multiple systems that do not talk to each other
- Interfaces for the business that are not user-friendly or intuitive
- Disorganized and disparate data stores, making insights difficult to generate
- Not having real-time analytics and monitoring, leading to missed anomalies

ABOUT CASE IQ

Case IQ offers an end-to-end compliance and case management solution that consolidates compliance monitoring, whistleblower solutions, third-party risk oversight, investigative case management and compliance approval and disclosures workflows. Lextegrity was acquired by Case IQ in 2025 and is now offered as an end-to-end suite of compliance tools.

Case IQ's software has been before enforcement agencies globally in 12 separate company engagements and was even recognized by the SEC as a remediation factor in a client's FCPA resolution. It has been chosen by several companies after the appointment of compliance monitors or after the start of an investigation and has been a factor in resolving those matters, including helping to secure a DOJ declination.

Case IQ

LEARN MORE

Request a demo today or explore how Case IQ can streamline your processes.
Visit www.caseiq.com or scan the QR code.

sales@caseiq.com | (800) 465-6089