

EXPERT GUIDE

Compliance Data Analytics: What does the DOJ expect?

An interview with Hui Chen, Compliance Counsel Expert at the U.S. Department of Justice (2015-2017).



Hui Chen

Hui Chen served as the first-ever Compliance Counsel Expert at the U.S. Department of Justice, where she was the exclusive consultant to federal prosecutors in the Fraud Section on evaluating corporate ethics & compliance programs. She is the author of the Fraud Section's "Evaluation of Corporate Compliance" – predecessor to the Criminal Division's Guidance on the same, which has served as an essential resource for compliance practitioners around the world. Prior to being retained by the Department of Justice, Hui served as a senior compliance leader in technology (Microsoft), biopharmaceuticals (Pfizer), and financial services (Standard Chartered Bank). Hui is also a contributing author to the recent Cambridge University Press book on Measuring Compliance, where she specifically addresses how legal and regulatory regimes measure compliance effectiveness.

Welcome, Hui. With your wealth of experience from various perspectives, we're excited to get your insights on how compliance data analytics should be used to meet the Department of Justice's expectations, with the standard government official disclaimer that you are speaking on behalf of yourself and not any current or past employer.

HUI CHEN: Thank you for having me. And yes, that standard disclaimer applies.

1. As an overview, can you discuss what the Department of Justice expects when evaluating a company's compliance program?

Sure. The Department of Justice asks three key questions when evaluating corporate compliance programs. First, the department wants to know if a company's compliance program is well designed. Second, the department considers whether the program is adequately resourced and capable of functioning effectively. Third, the department questions whether a company's compliance program is working in practice.

There's no single solution for companies seeking to meet these expectations, but integrating data analytics into your compliance program is a good place to start. Prosecutors want to see evidence to back up claims, and data – rather than presumptions and opinions – offer the most objective and verifiable evidence.

2. You've previously spoken about the need for companies to use data in compliance, but compliance has not been traditionally viewed as a data-driven field. What are your general observations on where most compliance organizations are today with respect to understanding their company's data?

Although there is growing interest in using data, most compliance departments have remained at the very rudimentary level in terms of data analytics. Most importantly, most compliance departments are not in the habit of monitoring their company's business data, such as their enterprise financial data, for compliance risks.

I recall a discussion I had with a Fortune 100 high-tech client whose compliance officer insisted that her company didn't have data on the marketing money being spent on distributors and data about the revenue those distributors were bringing in. The fact that she believed that was astonishing to me: these are basic kinds of data that every company needs to run its business. Understanding business data is the first step in understanding business, and understanding business is a fundamental necessity in order to be effective in driving compliance.

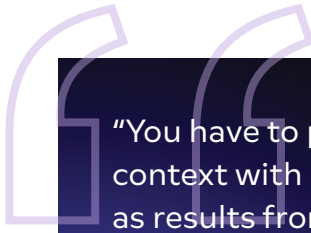


"Compliance organizations often rely on basic data like the number of investigations that are open or substantiated and the distribution of those cases in each country. Just looking at such raw numbers doesn't tell you very much."

3. When people hear the word "data," they often assume you're talking about numbers. But what does data analytics mean to you?

Data simply means information, and data analytics is about making sense of information: It's about trends, patterns, and outliers. For example, compliance organizations often rely on basic data like the number of investigations that are open or substantiated and the distribution of those cases in each country. Just looking at such raw numbers doesn't tell you very much. For example, you wouldn't immediately know whether having a low number of open or substantiated cases is good or bad because the number itself doesn't tell you that. A low number of open or substantiated cases might be due to people being scared to report matters or poor investigative capacities.

You have to put that data in context with other risk data, such as results from monitoring and auditing transactions in that same market. So, if you are finding a lot of noncompliance in your monitoring efforts in that same country, then you know your investigation numbers are not a reliable barometer of reporting. Even if you have substantiated investigations, more widespread monitoring and testing of transactions might even show you that your problems are more serious or widespread than the issues uncovered in those matters, or that your investigations have not been sufficiently thorough.



"You have to put that data in context with other risk data, such as results from monitoring and auditing transactions in that same market."

4. Companies frequently rely on raw data points and KPIs for identifying risks in their payments and disbursements, like the top travel and expense spenders, vendors with the largest invoices or distributors with the largest margins. What are the limitations of those kinds of raw data points and KPIs?

Many companies do top 10 or top 20 lists of different spend categories or in different vendor categories. For example, many compliance and audit teams focus on lists for the top travel and expense spenders in their company, but that might just confirm that the CEO has the highest T&E every month, which isn't very illuminating. Or a compliance team might look at the top 10 largest invoices for customs brokers in a high-risk country.

Looking at the top 10 or 20 is a start that can only get you so far, because the spend amount is just one of many factors of risk that should be looked at simultaneously to surface your highest risk behavior. For example, your highest risk vendor in that customs broker category might be in the middle of your spend distribution, but their invoice payments are frequently expedited, paid to an offshore bank account, always in round values and their address matches an employee's home address. That sort of multi-dimensional risk analysis using multiple data sets is where compliance data analytics need to go.



"Our highest risk vendor might be in the middle of your spend distribution, but their invoice payments are frequently expedited, paid to an offshore bank account, always in round values and their address matches an employee's home address. That sort of multidimensional risk analysis using multiple data sets is where compliance data analytics need to go."



"The fundamental question that I have advised prosecutors to think about when evaluating a company's compliance program is whether the compliance program is using data analytics like the rest of the company."

5. With all of this in mind, does the Department of Justice actively expect companies to use data analytics in their compliance programs?

Absolutely. Regulators and law enforcement have seen compliance programs with data analytics like the ones I mentioned above and have gone to academic conferences to see the latest research on compliance data analytics. They're also doing data analytics themselves. The fundamental question that I have advised prosecutors to think about when evaluating a company's compliance program is whether the compliance program is using data analytics like the rest of the company.

I can hardly think of any major companies that don't use data analytics in some way. If a company is using data analytics to make money, such as tracking and predicting customer behaviors, but isn't using data analytics to prevent wrongdoing, that seems like a deliberate choice to blindfold compliance. Companies can't say that they don't know how to use data analytics because it's already being used in departments other than compliance.



"If a company is using data analytics to make money, such as tracking and predicting customer behaviors, but isn't using data analytics to prevent wrongdoing, that seems like a deliberate choice to blindfold compliance."

6. To get a bit deeper on this subject, let's break down how data analytics can be used in compliance to meet the Department of Justice's three key aforementioned expectations. First, can you discuss how the department knows if a corporation's compliance program is well designed?

Yes. The department has singled out risk management processes and risk-tailored resource allocation, among other factors, as key things to consider when evaluating a compliance program. When judging a program's risk management process, prosecutors are considering what information and metrics – in other words, data – companies are using to help detect forms of misconduct. As mentioned, basic top 20 lists and other raw data points are insufficient tools to actively detect misconduct. However, data analytics using multiple data sets can provide genuinely impactful insights that can uncover patterns and trends that might have otherwise gone unnoticed.

As for risk-tailored resource allocation, one indicator is when a company devotes a disproportionate amount of time to monitoring low-risk areas instead of high-risk areas. For example, many compliance departments love to focus on travel and entertainment expenses which average maybe \$100 per transaction, while they fail to pay attention to third party payments that are tens of thousands per transaction. Another example is a client who told me that 80 percent of their third-parties are designated as high-risk through their due diligence process, which causes that designation to lose all meaning. They got to this point because the company's different departments were risk rating third-parties differently in their manual and subjective diligence process. This could've been avoided if the company relied more heavily on objective data from their financial systems, rather than solely the subjective data from their due diligence processes, to ensure it was monitoring the targeted third parties for different types of risks.

"Traditionally, companies emphasize due diligence in managing third-party risks. Due diligence, however, is only the first step in that risk management. The risk doesn't just come from who they were when they were onboarded: they come from what the third parties do with your company on a continuing basis. An adequate compliance program needs to follow robust onboarding processes with active ongoing transaction monitoring."

7. You've previously been very vocal about the limitations of companies' current approaches to third-party risk management. Does the Department of Justice emphasize the importance of effective third-party management when evaluating a company's compliance program?

We need to remember that the Department of Justice evaluates compliance program in the specific context of their prosecutions. Given the frequency with which third parties have played a role in corporate criminal activities, that is one area that constantly comes under scrutiny. Traditionally, companies emphasize due diligence in managing third-party risks. Due diligence, however, is only the first step in that risk management. The risk doesn't just come from who they were when they were onboarded: they come from what the third parties do with your company on a continuing basis. An adequate compliance program needs to follow robust onboarding processes with active ongoing transaction monitoring.

I often give this analogy: if you just do due diligence and don't do anything afterward, it'd be like a credit company that checks your credit score before issuing you a card, then never monitors your card activities afterwards. Do you know any credit card company that works like that? Credit card companies have the ability to monitor all user transactions in real-time. Now, the question is, "Why are we not using the same kind of continuous transaction monitoring in compliance?"



"If you just do due diligence and don't do anything afterward, it'd be like a credit company that checks your credit score before issuing you a card, then never monitors your card activities afterwards. Do you know any credit card company that works like that? Credit card companies have the ability to monitor all user transactions in real-time. Now, the question is, 'Why are we not using the same kind of continuous transaction monitoring in compliance?'"

8. How important is it to the Department of Justice for companies' compliance programs to be based on objective, data-driven information, rather than subjective decision-making?

It's extremely important. As I said, the Department of Justice is a prosecuting agency, and prosecutors want evidence. As I mentioned, a major limitation of traditional third-party risk management is that it relies on subjective decisions about what is high-risk or not. People think, "Well, for this type of risk we think that marketing vendors must be high risk, so let's categorize all marketing vendors as high risk." What is the evidence that all marketing vendors present the same level of risk? Broad categorizations based on nothing other than people's gut feelings is not a responsible way of conducting compliance.

On the other hand, data can provide a compliance team with objective evidence and assessments about their company's risks, including third-party risks. This shows prosecutors that your company is committed to evidence-based risk detection and proactively detecting wrongdoing, which is what prosecutors are used to.



"On the other hand, data can provide a compliance team with objective evidence and assessments about their company's risks, including third-party risks. This shows prosecutors that your company is committed to evidencebased risk detection and proactively detecting wrongdoing, which is what prosecutors are used to."



"A major limitation of traditional third-party risk management is that it relies on subjective decisions about what is highrisk or not."

9. As for the Department of Justice's second expectation, how do prosecutors determine if a compliance program is adequately resourced and empowered to function effectively?

The Department of Justice has specifically cited data resources - and access to that data - as a key component of this question. Prosecutors expect companies to use data to demonstrate that compliance resourcing is proportionate to the risks presented by the company's business profile. This means the evidence about resourcing and effectiveness must be built on data relating to the company's business model and operations.

Data analytics is about putting the pieces of the puzzle together. It's the big picture, not the raw data. All of the interesting data, when it comes to compliance, comes from the business data, aside from investigations data. The team that puts it together and tells a story that impacts business decisions will be valued in the company. If I were a compliance person, I'd want to be the one to paint this narrative and inform the business about what issues the company should prioritize from a risk mitigation perspective. That data is sitting in companies' financial systems and business systems. It's already there.

"Data analytics is about putting the pieces of the puzzle together. It's the big picture, not the raw data. All of the interesting data, when it comes to compliance, comes from the business data, aside from investigations data. The team that puts it together and tells a story that impacts business decisions will be valued in the company. If I were a compliance person, I'd want to be the one to paint this narrative and inform the business about what issues the company should prioritize from a risk mitigation perspective. That data is sitting in companies' financial systems and business systems. It's already there."

10. How can companies ensure that their compliance programs are working in practice?

Ensuring that your company's compliance processes are actually being used and fostering a culture of compliance are key. On the former point, people are used to things that are user-friendly in their daily lives and have less and less patience with unnecessary or clunky systems. You can't blame the user. You need to think about whether your process actually reduces risk and, if it does, whether the process or tool is intuitive and integrated into the business users' everyday work life.

Beyond that, implementing consistent testing of your program is the best way to ensure that your program is working effectively in practice. Metrics like hotline reports, training stats, code of conduct certifications are often self-selected and extremely limited in what they reveal, and can provide a false sense of security about your program. Typical fraud schemes can go on for months or years before anyone reports something, if they do at all, and the participants in those schemes are clever enough to complete their training and annual certifications with no qualms.

Compliance organizations that use data analytics to independently test 100% of their financial transactions for non-compliance, ideally globally and in realtime, have the clearest picture of whether their programs are actually operating effectively - a picture based on data rather than hearsay.

"Using data in compliance isn't just about 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."

11. Though the Department of Justice expects companies to leverage their data in their compliance programs, companies remain hesitant about investing in compliance data analytics. How would you convince companies to take the plunge?

Using data in compliance isn't just about 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 doing 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 real data that shows them their spend and their risk and can 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.

"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 samplebased audits."

"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."





"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 real data that shows them their spend and their risk and can 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."

12. Do you recall any specific instances in your career where data could've been used to save companies time and money?

I remember very clearly from my time at the Fraud Section when a corporate monitor came in to present his findings on a company. There was an issue with this particular company about the use of corporate credit cards and the monitor recommended that the company train all of its employees on the use of corporate credit cards. It turned out that there were only around 200 people at the company who had corporate credit cards. This monitor was going to make compliance train tens of thousands of people for something that was only relevant for around 200 people! Talk about an utter waste of money, time, and resources - not to mention the damage to the credibility of the compliance department in this case.

If the monitor and the company simply looked at the data underlying the problem, they would've seen that probably only a subset of those 200 people, such as those who use the corporate credit cards for certain types of transactions, actually needed training. That would have saved the company from making a significant and unnecessary investment in training. This is why I urge compliance professionals to really think about how they're using their data and ensure they are being judicious in their use of resources.

13. That's an interesting example of how data could have benefited a company. Do you have any specific examples where compliance teams actually did use data to save their companies money?

Several years ago, I spoke to a compliance professional whose company had just started to use data analytics. The business had been advised of the risks of a certain type of marketing event, but the business owner was unconcerned. This compliance professional, armed with the business's financial data, showed the business owner the cumulative spend for these marketing events. Turned out the business owner had never focused on the cumulative cost of these events: he was shocked by the amount and decided to shut the events down because of the poor return on investment. So, the owner was probably more motivated by not wasting money, rather than the potential compliance risks the events were causing, but that doesn't matter. It's the result you want. That situation raised the business' interest in using compliance data analytics to manage risk.

"What's there is there: you can choose to ignore it or use it. Data is not privileged and there is no way a company can claim that it is."

14. Even when considering the financial incentives of compliance data analytics, sometimes in-house teams are concerned that using data analytics will open a "Pandora's box" of issues that need to be followed up upon. To close things out, how would you respond to compliance teams that have that concern?

I don't know how that attitude is different from plugging your fingers in your ears. What's there is there: you can choose to ignore it or use it. Data is not privileged and there is no way a company can claim that it is. So, do you really want to wait until the Department of Justice or another law enforcement agency comes in and dives into your data and tells you troubling things about your company that you could've uncovered five years ago but chose not to?

15. So, to be clear, is it better for companies to be proactive in their risk detection and management?

Absolutely. It is better that you know what's in the Pandora's box rather than a prosecutor opening it and turning around to you and saying, "You could've found these issues several years ago and resolved them. Instead, you have let this sit there and fester and now it is a much worse problem because you have purposely ignored having this data and doing anything with it." As mentioned, the Department of Justice expects companies' compliance programs to be able to present evidence of effectiveness in preventing and detecting misconduct. Taking a proactive approach by using compliance data analytics meets those expectations.

"It is better that you know what's in the Pandora's box rather than a prosecutor opening it and turning around to you and saying, 'You could've found these issues several years ago and resolved them. Instead, you have let this sit there and fester and now it is a much worse problem because you have purposely ignored having this data and doing anything with it.'"





"The Department of Justice expects companies' compliance programs to be able to present evidence of effectiveness in preventing and detecting misconduct. Taking a proactive approach by using compliance data analytics meets those expectations."

16. Wonderful. One last question for you: at Lextegrity*, our approach to risk management combines doing due diligence prior to contracting, through our approvals and disclosures and third-party management software. But then goes beyond that to enabling risk scoring of 100% of your financial transactions, whether travel expenses, vendor invoices or customer/distributor transactions, using sophisticated and configurable behavioral, statistical and policy-based forensic analyses.

We are proud that our software was cited by the SEC in one of our client's FCPA resolutions as a significant remediation item and was a factor in that client also receiving a DOJ declination. But can you describe how you would have viewed a company that used technology like this when you were with the DOJ?

I would have viewed Lextegrity's approach of managing risk across the life-cycle of spend – from the due diligence process through the spend process itself – very favorably. A technology and approach that tests the entirety of your financial transactions using multiple risk analyses simultaneously provides a much higher degree of comfort around whether your program is actually operating effectively than doing due diligence only or relying only on infrequent sample based auditing to supplement your diligence. In fact, a handful of companies have implemented exactly this approach and shown it to the DOJ over the years and prosecutors know first-hand what is now possible and will continue to expect organizations to up their game and implement solutions like that.



"I would have viewed Lextegrity's approach of managing risk across the life-cycle of spend – from the due diligence process through the spend process itself – very favorably. A technology and approach that tests the entirety of your financial transactions using multiple risk analyses simultaneously provides a much higher degree of comfort around whether your program is actually operating effectively than doing due diligence only or relying only on infrequent sample based auditing to supplement your diligence. In fact, a handful of companies have implemented exactly this approach and shown it to the DOJ over the years and prosecutors know first-hand what is now possible and will continue to expect organizations to up their game and implement solutions like that."

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

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

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

