Brought to you by the publishers of COMPLIANCE WEEK

What factors are driving change in your CORPORATE INVESTIGATION processes?

An e-Book publication sponsored by opentext™

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is a business intelligence and information service on corporate governance, risk, and compliance that features a daily e-mail newsletter, a bimonthly print magazine, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for chief compliance officers and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance practitioners. www.complianceweek.com

opentext™

OpenText provides Enterprise Information Management software that enables companies of all sizes and industries to manage, secure and leverage their unstructured business information, either in their data center or in the cloud. Over 50,000 companies already use OpenText solutions to unleash the power of their information. To learn more about OpenText (NASDAQ: OTEX; TSX: OTC), please visit www.opentext.com.

Getting to the core of your investigations

The results of a recent survey from Compliance Week and OpenText reveal that while investigations and data volumes are on the rise, machine learning combined with external expertise may give companies the upper hand in accelerating response and results, writes **Jaclyn Jaeger**.

Numerous companies still rely on inefficient, manual processes when conducting investigations, resulting in wasted time and resources. And yet, many compliance officers and in-house lawyers would tell you the challenges that come with the rise in the number and types of investigations.

That's the finding of a recent cross-industry poll from Compliance Week and information management software provider OpenText, the "Investigations benchmarking survey," that polled 200 compliance, audit, legal, and risk practitioners on: how they view the investigative process within their companies, what has changed in the process during the last few years, what to expect in the future, and much more. Respondents were from the following functions: Legal (14%); Risk Management (10%); Internal Audit (18%); Compliance (42%); HR (3%); IT (1%); and Security (4%), with 8% choosing "Other." Most respondents (65%) selected the compliance function within their organization as having primary responsibility for overseeing investigations, closely followed by legal (54%).

The survey said 51 percent of respondents expect the number of investigations at their companies to increase over the course of the next one to two years. Another 41 percent of respondents expect no change, while 8 percent project a decline.

"Incident response, in particular, is a growing source of both forensic and ESI investigations, as more and more organizations experience security breach and cyber-security threats."

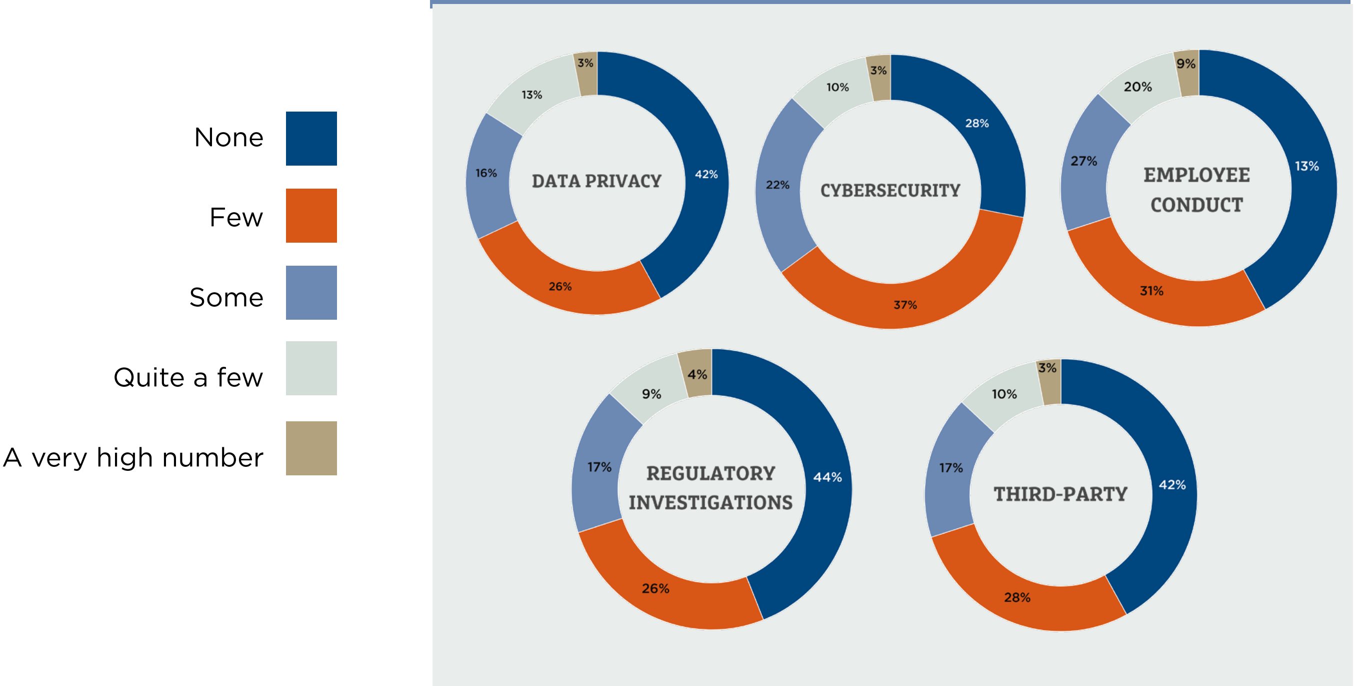
Tom Gricks,
Lead Strategy Consultant,
OpenText

Types of investigations increasing

Breaking it down even further, the survey reveals which investigation categories are top of mind for those polled. Data privacy, cyber-security, third-party C-suite vetting, and regulatory investigations ranked high on the list.

Survey respondents indicated that they face several types of investigations, further

What type of investigation(s) did your organization face in the past year?
Please rate each by predominance/volume relative to the total number of investigations.



stressing the need for automated processes. According to the survey, the top three types of investigations they face relate to employee conduct, cyber-security, and regulatory investigations. Twenty-nine percent said that employee conduct issues generate "quite a few" to "a very high number" of investigations, while 16 percent said the same for data privacy, 13 percent for cyber-security and data breaches, and 13 percent for regulatory investigations. Other types of investigations concern third parties, financial reporting/securities, COVID-related fraud, and intellectual property/trade secrets.

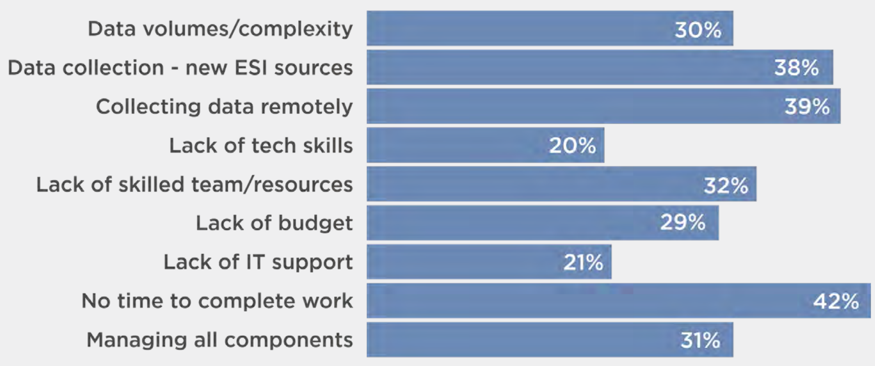
"Incident response, in particular is a growing source of both forensic and ESI investigations, as more and more organizations experience security breach and cyber-security threats," says Tom Gricks, lead strategy consultant for OpenText. "Organizations must be prepared to expedite the isolation, itemization, and analysis of all manner of data, including both personal data such as PII and PHI, as well as commercially sensitive documents."

Paint points/business challenges

The plurality (42 percent) of those polled said their biggest pain point in managing and conducting investigations is "not enough time to complete work with available resources," and yet 46 percent responded they expect their budget for investigations to remain the same. Another 12 percent said they expect it to decrease. In response to another question, 76 percent of respondents said they are still employing manual review.

42% of respondents said their biggest pain point in conducting an investigation is **"not enough time to complete work with available resources,"** yet 29% **lack budget** and 76% still **employ manual review.**

What do you believe are your organization's biggest pain points in terms of managing and conducting investigations? (Select all that apply.)



Other common pain points cited by respondents included "collecting data from remote and/or off-network locations" and "difficulty collecting data from new sources of electronically stored information (ESI)," each coming in at 39 and 38 percent, respectively. Following those were "lack of a skilled team" (32 percent) and "volume and complexity of data" (30 percent).

Compounding these problem areas is the archaic way many companies are still conducting investigations. Specifically, 76 percent of respondents said their investigation teams still perform a manual review to identify key documents in an investigation. Just 30 and 31 percent, respectively, said they use advanced analytics machine learning, such as technology-assisted review, and only 7 percent reported using artificial intelligence (AI) capabilities.

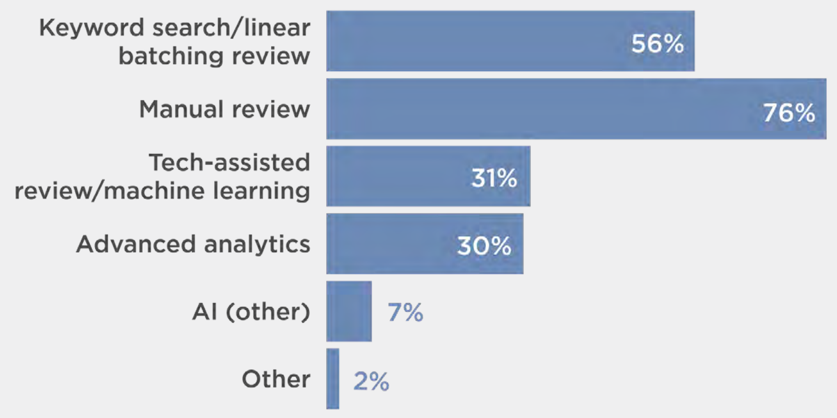
Purchasing decisions

The survey also queried respondents on who was responsible for purchasing decisions in terms of investigations technology, with 30 percent noting that duty belonged to legal followed by compliance at 22 percent and IT at 17 percent. When asked whether the same person was responsible for hiring third-party providers for investigations support, a significant 83 percent said yes.

In answering where the biggest chunk of their investigation spend is allocated, 62 percent of respondents said toward "consulting services" and/or "legal service providers," while 40 percent said law firms. Among the reasons respondents gave for hiring third-party service providers included for forensic purposes; to do electronic discovery (e-discovery); to help evaluate personally identifiable information; and to provide expertise the company does not have.

> Among the reasons respondents gave for hiring third-party service providers included for forensic purposes; to do **electronic discovery** (e-discovery); to help **evaluate personally identifiable information**; and to **provide expertise.**

Which approaches does your investigation team typically use to identify key documents in an investigation?
(Select all that apply.)



> "Data analytics, automation, and machine learning are necessary tools in supporting investigations that involve large amounts of electronically stored information."
>
> Andy Teichholz,
> Global Industry Strategist,
> Compliance & Legal, OpenText

How is technology being utilized?

Collectively, the findings demonstrate many companies are not leveraging the sort of data analytics, technology-assisted review, and AI capabilities that would expedite investigations while saving valuable time and limited resources. "Data analytics, automation, and machine learning are necessary tools in supporting investigations that involve large amounts of electronically stored information," says Andy Teichholz, global industry strategist, compliance & legal at OpenText.

Most investigations today involve massive amounts of ESI, including the need to engage in data analysis and review associated with regulatory investigations, cyber-security/data privacy compliance, financial reporting, and employee misconduct, Teichholz notes. These issues have only been heightened by the pandemic and remote work realities. According to the survey findings, two of the top issues most likely to lead to an investigation were cyber-security and data privacy.

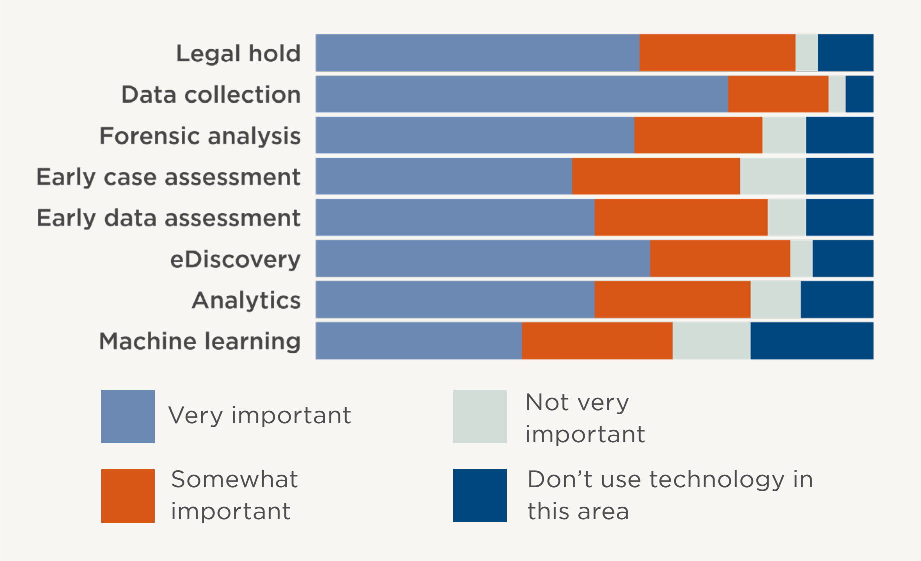
Additionally, survey respondents indicated that the top three types of investigations that generate the most amount of electronically stored information (ESI) for collection and review were employee conduct (37 percent), cyber-security and data breaches (35 percent), and regulatory investigations (34 percent).

The survey notes that more than half of respondents (52 percent) said that more than 25 percent of their ESI investigation activities involve document review, and 76 percent of respondents are still performing that type of review manually.

The survey breaks down technology's role in supporting various investigatory functions, including data collection, which 74 percent of respondents deemed very important. Following was e-Discovery (60 percent), legal hold (58 percent), forensic analysis (57 percent), and a tie between analytics and early data assessment (50 percent). (See below for a full breakdown of respondents' answers).

52% of respondents said more than a quarter of their company's ESI investigation activities involve **document review.**

For each of the functions below, how important is technology in supporting investigations? (You can select the same level of importance for multiple functions)



Other areas of focus

Investigations related to "C-suite vetting" were cited by respondents as another key area of focus. Many modern companies recognize hiring senior executives demands a more vigorous vetting of candidates, "because there is so much scrutiny today on everything that the C-suite does," says Gricks.

Especially for large, well-known companies, a senior executive's words or actions don't even have to be criminal or fraudulent in nature to come under scrutiny. "It may simply be a proclivity that leads someone looking from the outside in to be critical of that individual's background," Gricks says.

The survey findings also reveal that in addition to private complaints and proactive compliance monitoring, whistleblowers are still an important trigger of an investigation. "53% of respondents ranked whistleblowers as a typical investigation trigger." And Teichholz expects this number should significantly increase as well. "Whistleblowers are being encouraged, protected, and incentivized with financial awards more than ever before," he says. "Expect to see even more investigations in the future triggered by whistleblowers as a speak-up culture is being embraced around the world."

Litigation risk and investigative approach

According to the findings, the top three issues that "almost always" result in litigation are those that stem from regulatory investigations or enforcement, trade secrets, and financial reporting. Following closely behind were issues having to do with data privacy compliance, employee conduct/workplace issues, and cyber-security/data breach matters.

"The conclusion of an investigation is increasingly unlikely to mark the end of the matter,” says Tracy Drynan, a senior consultant at OpenText. Especially if the matter becomes public, the company can face follow-on actions brought by customers, third-party suppliers, or former employees, she says.

Reducing litigation risk—or better managing it—begins with conducting a thorough investigation from the get-go, Gricks says. Yet, as the findings revealed, many companies still rely on dated processes that are holding them back from conducting truly thorough and robust investigations.

“Companies really haven’t made the transition to a true investigative approach,” he says.

For legal and compliance teams, what that means in practice is recognizing data analytics and technology alone do not make for an effective investigation. “You need experienced individuals who can drive the analytics,” Drynan says.

Prudent companies today leverage what Drynan refers to as an investigatory “strike

> “The conclusion of an investigation is increasingly unlikely to mark the end of the matter.”
>
> Tracy Drynan,
> Senior Consultant,
> OpenText

Why outsource?

Respondents were asked their main reason for using third-party service providers. Here’s a snapshot of their answers.

For audits that require external party review

When additional expertise is needed

For specialized services such as forensics

In eDiscovery for privacy regulations

For large, complex cases

With incoming third-party PII evaluations

When the required skills are not available internally

If compliance department is overwhelmed by regulatory issues

For artificial intelligence and machine learning purposes team," which she describes as a small, elite group of three or four people "fluent in technology and analytics" who know how to hunt for answers in the data in an intentional way.

Of course, a true investigation differs from a document review—the kind legal teams employ for e-discovery, for example—which doesn't necessarily piece together all facts and evidence in a way that tells a complete story, Drynan says. A strike team, by comparison, essentially lives and breathes the data day in and day out, connecting the dots between all evidence and documents, even those that initially seem unrelated or irrelevant, she explains.

In essence, a strike team complements in-house counsel, compliance, and audit because, by surfacing the key facts, it enables the company to better inform what direction an investigation should take; what witnesses to interview; whether to self-report a matter; or where remediation efforts may be needed, for example.

> "The survey findings also point to the multidisciplinary aspect of investigations today, which is consistent with some of the trends we have been seeing over the past few years. Between the proliferation in global data privacy regulations, rising cyber-threats, and more companies going digital, all these factors combined have resulted in companies taking a more cross-departmental approach to investigation management and execution."
>
> Andy Teichholz, Global Industry Strategist, Compliance & Legal, OpenText

Risk functions collaborate

The survey findings also point to the multidisciplinary aspect of investigations today, which is "consistent with some of the trends we have been seeing over the past few years," Teichholz says.

Between the proliferation in global data privacy regulations, rising cyber-threats, and more companies going digital, all these factors combined have resulted in companies taking "a more cross-departmental approach to investigation management and execution," he says.

What we're seeing now is a convergence in the collaboration between risk functions—including compliance, risk, legal, audit, HR, security, and IT. Each role brings to the table expertise that informs or touches upon the objectives and priorities of other departments, "including findings that indirectly help identify other vulnerabilities to address broader policy, process, or system problems," Teichholz says.

The more interconnected all of these various departments and the more they provide value to each other, the more effective investigations and risk mitigation will be. ■

opentext™ | Recon

Expedite investigations with rapid insights

Speed up compliance investigations using OpenText™ Recon

- Get the facts early to make strategic case decisions and optimize outcomes
- Centralize on a single vendor to eliminate inefficiencies
- Reduce the time and cost of an investigation

Recon is a seamless, end-to end managed service that brings together people, technology and process to speed up your investigations.

Visit opentext.com/recon-investigations today