Voices Computer code can make IT audits less painful

By **Corey Scobie**
Published **January 30 2019, 1:42pm EST**

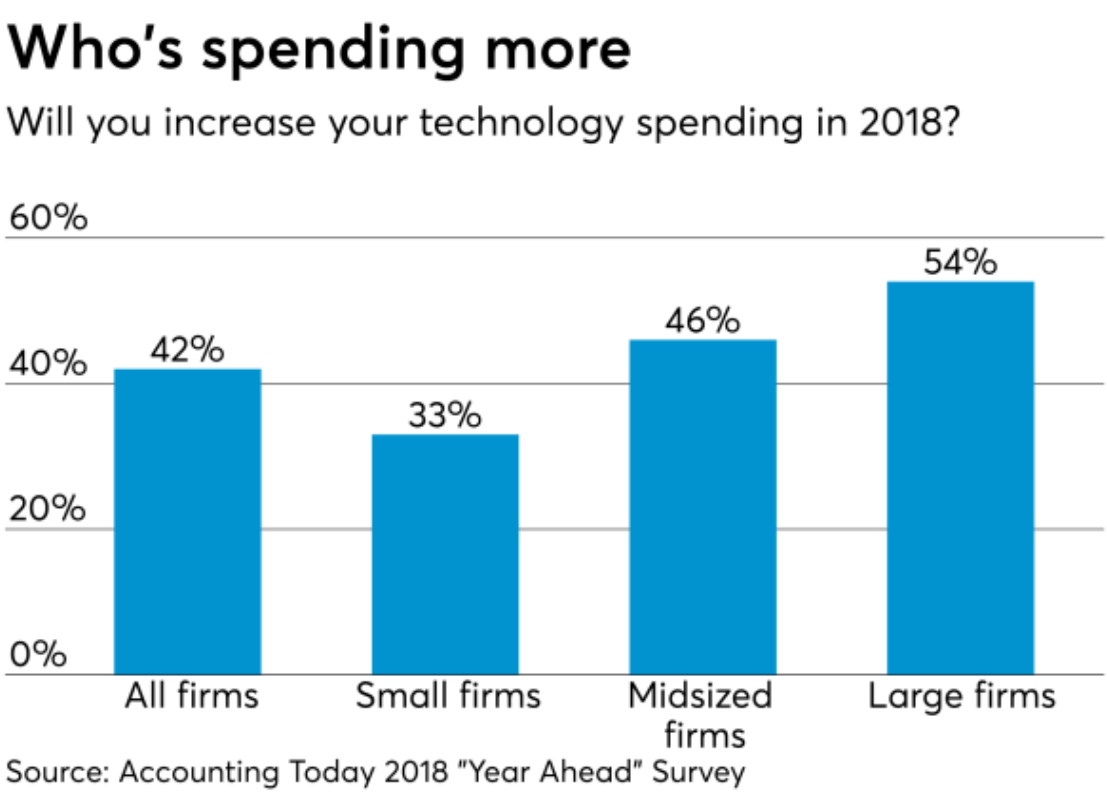
More in **Compliance systems, Data and information management, Data governance, Compliance**

Your quarterly or semi-annual financial audit looms. Your team is frantic. They must collect all bank transaction data from bank accounts, accounts payable and receivable data from your payment systems, expense report information for employees from another system, and Forex exposure from yet another system.

What's more, they have no idea whether the data is accurate or reliable. The dirty secret is, you had no control over quality and collection of your financial data. No systems would automatically flag and refuse a reimbursement request for an employee buying cases of Dom Perignon champagne and shipping them to their house. You can't spot anomalous Forex patterns in your Eastern European Forex hedging, so you blindly accept all the Forex data. You know there are no controls, really, but you just hope that's not a problem and your company doesn't get hit with a massive fine or a nastygram from the Internal Revenue Service.

Then your team takes all that data you painstakingly collected manually and puts it into...a spreadsheet or a PDF.

Now, anyone who understands how the financial world works knows that sophisticated Enterprise Resource Planning (ERP) software puts in place full controls, reliable data collection, and repeatable processes for auditing and audit trails. To a modern CFO or head of accounting, the chaos I describe here sounds like madness.



Chaos, rinse, repeat

Unfortunately, this is a fairly accurate description of how IT audits work at most companies today. Every IT audit is a new snowflake of chaos with few repeatable processes, multiple systems of record and totally siloed audit trails of log files and records — and even email attestations — across software development, IT operations, developer operations, HR, and sales and marketing. Because the IT and security teams operate in a universe of code and data security that is very different from those of the finance and compliance teams, ensuring data quality and baking in controls on IT operations processes is like learning an entirely new language.

Aside from being stressful, IT audits are costly. Your costly IT and software development teams spend weeks chasing down answers to audit questions and not performing revenue-generating work. Your company audit team spends a disproportionate amount of time doing tedious tasks, collating emails and PDFs into consumable reports.

This is only during the audit. After the audit is completed, how can you be sure that your organization is not falling out of compliance again? There is no way to know. And that constitutes a major risk to your firm — a security risk, a financial risk, and a regulatory risk. So not only was compiling the audit painful; there was no way to observe whether compliance was maintained between audits.

Cloud computing, automation and new opportunities

Let's consider, for example, payment card industry compliance, a common requirement for many businesses today.

In the past, PCI compliance was tightly tied to a manual auditing process and an inflexible relationship with a few trusted outside entities such as payment processors. In modern cloud scenarios, the payment processor — say, Stripe, a well-known payments processing engine — can be one of any number of payments processors integrated into the process as a JavaScript snippet included in application code. That snippet may reside in any geographic location on Earth, in any number of cloud data centers, and its location may move multiple times in an hour, let alone a day. The application that feeds data into the Stripe JavaScript snipped may be on any number of domain names and may or may not have gone through a rigorous security audit to ensure that customer data is safe. The customer information feeding into that Stripe snippet could come from any number of databases stored in the cloud that a company is relying on, or from third-party databases if the customer is referred in via a partner.

Consider the moving parts factored into an IT audit. First, the physical compute infrastructure is constantly changing. Second, the applications where the PCI-compliant process may reside are difficult to track due to distributed development teams. Third, there may be multiple systems that connect to and feed into the PCI-compliant process so a breach in any of those systems — third-party or internal — will violate compliance.

"Compliance-as-code": The modern path to always-on IT auditing

The good news? The manual processes described above involved in managing not only the PCI compliance but compliance in general can be automated via software code. This shift to automation opens up a blue ocean for monitoring and enforcing compliance on a continuous basis — the mythical "push-button IT audit" and what we call "compliance-as-code."

Compliance-as-code can be baked into the foundation of cloud-based IT infrastructure. In the same way that developers can add Stripe snippets to applications, IT audit and security teams can append "audit snippets" to every software process and virtual infrastructure component. The snippet as the proxy and auditor of events in IT infrastructure is accepted. For example, application performance monitoring (APM) inserts snippets (called agents) alongside databases, web servers

and infrastructure. The snippets report performance statistics to ensure the delivery high-quality digital experiences and feed information into dashboards – and databases used for audit trails.

These types of capabilities can make IT audits nearly automatic, affording your team confidence that compliance rules are instrumented as code and actively preventing and reporting compliance breaches.

Compliance-as-code is not only possible but comparatively easy compared to the frantic fire drill status quo. No more emails flying around, no more cumbersome PDFs and no more manually-updated spreadsheets to codify IT audits. With compliance-as-code, IT auditing resembles reliable and repeatable processes in finance like ERP systems, and turn error-prone manual processes into predictable, push-button workflows.

Corey Scobie