

Five Ways to Reduce Your Audit Tax

Taxes are certainly not fun, but there is something worse: an audit. Combine the two in a risk and compliance scenario and you have the onerous “audit tax,” a figurative term used to describe the expenses a company incurs when deploying resources and manpower to satisfy the burgeoning set of internal and external compliance and audit mandates.

The good news is that there are ways to reduce the audit tax burden. This whitepaper outlines five methods organizations should consider to streamline their compliance efforts and thereby reduce their audit tax.

Introduction

The security and regulatory environment these days has mushroomed to the point that very few organizations go untouched by the auditor's viewfinder. In fact, most midsize to large enterprises engage in so many compliance activities that it may seem as if they are endlessly undergoing one audit cycle or another. For these organizations the high cost of compliance is unavoidable. In effect it has become a sort of "tax" on the enterprise. This audit tax manifests itself in a number of ways. Organizations pay it when they divert personnel and manpower to prepare for audits and liaise with internal and external auditors. They pay the tax when they hire expensive consultants to assist in the effort. Some pay the audit tax in the extra time spent by auditors sifting through missing information and undergoing a second audit after a failed first attempt.

Even though no organization can completely sidestep the audit tax, it is possible to pay less than the competition. Management must apply the old "Work Smarter, Not Harder" philosophy to compliance efforts to cut down on compliance costs and reap the greatest security benefit for the money invested.

The following five methods offer a good start toward reducing the business audit tax to a manageable line item.

1. Take a Top-down Approach to Compliance

Too many organizations pay far too much for audit activities without IT leadership even having a clear picture of the total money spent. What's more, they often shell out compliance money without any true visibility into the overall risks facing the organization and no way to know whether disparate compliance expenditures truly mitigate these risks. Not only is visibility poor in these cases, but these enterprises ultimately pay a higher price for compliance as a result.

The problem right now is that many companies try to comply without a comprehensive strategy. Disparate teams are responsible for completing compliance activities within their confined business processes and technology. Operating within technological silos, team members often don't know how their activities fit within the overall compliance picture (and sometimes they don't even care). They have no clue how compliance and risk information overlaps, or whether they are covering any gaps in information that crop up between silos.

This kind of bottom-up approach to compliance drives up the audit tax and also leaves organizations more at risk. The approach is rooted in the fact that a lot of organizations fail to allow information security professionals to pull up a seat at the IT leadership table. They fail to employ any semblance of governance over information security teams to drive their efforts in a directed manner.

In the absence of this direction, enterprises fail to take a top-down risk management approach that strategically sweeps across the entire organization. Efforts are fractured and lack any kind of symmetry. Different subsets of IT and business groups, supported by information security, tend to follow their own brand of compliance procedures. Inevitably the wheel is invented more than once across the organization.

Taking a top-down leadership approach reduces the audit tax by eliminating these redundant efforts and offering an enlightened vantage point to direct manpower where it is needed and when it is really needed to comply with auditors' demands.

Most importantly, it offers IT leadership shared visibility into security activity across different business units and security groups to further improve risk management decisions. This not only helps streamline information security operations and reduce the cost of compliance, it also aids enterprises in complying with the spirit of most regulations, which are ultimately put in place to improve the overall security of organizations and their customers.

2. Harmonize Multiple Compliance Efforts

Compliance silos and stovepipes pop up all over the security and compliance landscape for two reasons. The first, of course, was mentioned in point number one. So many organizations tend to approach compliance on a business-unit-by-business-unit basis.

Many organizations also tend to drive up the cost of their audit tax by tackling compliance on a regulation-by-regulation basis. Different personnel and resources are directed to prepare for very specific regulatory audits with no lines of communication established to discuss each effort. Organizations overspend on point products for particular pieces of regulation, such as [PCI](#) or [HIPAA](#), that are unable to provide any kind of cross-regulation support.

Meanwhile, most security regulations have a great deal of overlap in philosophy and actual controls that beg to be exploited. Rather than operating within silos, compliance managers striving to meet individual regulatory demands need to compare notes and find ways to comply with multiple regulations using as few steps as possible. Similarly, teams need to take a look at product spending and ensure they are getting the most value from their investment in compliance solutions. The ideal compliance products should be able to aid the team in achieving positive results across multiple compliance initiatives.

The harmonization effort encompasses the three key elements of security: people, process and

technology. By bringing together the people responsible for compliance, having them discuss and strategize processes that will achieve multiple compliance goals at once, and by choosing products that can pull together information from numerous technology silos, the resultant harmonization will ultimately slash the bottom line.

3. Automate Compliance Data Gathering

A recent study by Internet Research Group, found that more than half (51%) of large organizations either use no tool at all or use spreadsheets. More than two-thirds (69%) of smaller companies either use no tool at all or use spreadsheets. Unfortunately, this practice ultimately causes these organizations to pay a much higher audit tax than their counterparts that are using automated data-gathering tools.

Spreadsheets are error-prone and depend on an extremely manual process. A company that is dependent on spreadsheet audit preparation likely has spreadsheets scattered all across the organization. Different business units likely use different formats to input data, as the organization likely has not employed a standard format. As disparate people touch the data, some faulty data is entered, and other important data is left out.

Most troubling about this process is that for each individual audit, these spreadsheet figures must be updated and validated. Whether done

in-house or by the auditor, this is a costly process. Implementing an automated compliance data gathering product gives companies the power to scan their environment once and report many times, better satisfying multiple regulation requests simultaneously.

Rather than manually sifting through individual vulnerability scanning products, policy auditing tools and configuration management products to find relevant data, an automated solution should be able to find the right information and analyze it in a meaningful way.

Similarly, automated tools should also be able to aid an organization with electronically generated surveys that track people and processes and provide risk scoring. Too many organizations take an ad hoc approach to survey administration, failing to standardize questions, forgetting to collect answers from all involved parties and operating in a disorganized fashion.

An automated solution can help define consistent questions, e-mail surveys and track responses to stay organized. By automating to the greatest extent possible, companies keep a lid on the amount of time billed by their auditors. Manual reporting almost certainly pushes out the length of the audit process, because if you take a manual approach to collecting data, the auditor will take a manual approach to hunting down and verifying the data stated on your report.

4. Apply Compliance Best Practices

When a company works off a higher standard of technical and procedural controls than what is mandated by an individual regulation, that organization tends to operate a more secure environment while handily satisfying most of the other regulations along the way.

While it might not be the easiest approach, the most effective way to reduce your audit tax is to take a long look at security standards such as CoBIT, ITIL or ISO27002 and adopt the best controls that work for your organization. Unlike many regulatory demands, which can often be vague and oblique, these best practices and security recommendations offer advice for actionable controls that will improve risk management and fulfill compliance needs all in one go.

True, it may take some extra time to identify the best controls for your environment, but it will help you to streamline your overall compliance process. Doing so may allow you to create a hybrid framework that pulls elements from multiple standards. No matter how you slice it, you should be sure to first examine your security and your regulatory requirements before selecting controls that are appropriate to your circumstances. By implementing controls laid out by these best practice frameworks, companies will not only reduce their audit tax, they'll achieve more accuracy in compliance reporting. Smart IT organizations are able to leverage regulatory compliance budgets into processes and technology that ultimately improve business security, efficiency and quality. It also helps IT demonstrate additional value by reducing audit costs, providing timely risk and compliance reports to management and auditors.

5. Learn to Deliver the Right Compliance Reports

Think about this for a moment: Would you rather pay your staff to complete a specific compliance activity, or would you rather pay an expensive auditor? Seems like a no-brainer, right?

Unfortunately, when an organization fails to validate their proof of compliance before an audit they end up paying expensive auditors to manually gather compliance data across the company. Companies that don't have a good understanding of the reports and proof necessary to certify compliance will see their audit tax go up. The less prepared an organization is, the longer an auditor will need to spend on-site gathering compliance information. More time means more billable hours before the auditor finally breaks out their rubber stamp.

Companies must work with auditors to figure out what information the auditors need to see and when they need to see it. From there it is possible to start trimming costs by getting IT and business users to work together to establish built-in, structured and repeatable reporting processes that satisfy auditors' demands. This can be done by pre-defining reports and queries based on what the auditor has told you. Then these reports can be scheduled to run at appropriate times and can be retrieved when the auditor requests them.

Ultimately, your organization wants to condense the auditor's time on-site. This can be achieved through proper communication with the auditor and by instituting the automation techniques mentioned in step three.

Five Ways to Reduce Your Audit Tax

While you can't eliminate the audit tax altogether, it is possible to reduce it and ultimately gain value out of the costs incurred. Your goal should be to bring together individual compliance activities under an overall corporate strategy that includes all segments, technologies and regulations with which the company must comply. A cohesive strategy with specific, non-redundant controls lends itself to greater automation of data gathering and more accurate reporting.

Beyond audit tax savings, this streamlined process gives a much better view into all of the risks facing the organization and provides an efficient means to making important mitigation decisions. Thus, an organization reaps meaningful benefits to their audit tax, rather than just considering it as another sunk cost.

Continued »

About Lumension

Lumension, a global leader in operational endpoint security, develops, integrates and markets security software solutions that help businesses protect their vital information and manage critical risk across network and endpoint assets.

Lumension enables more than 5,100 customers worldwide to achieve optimal security and IT success by delivering a proven and award-winning solution portfolio that includes Vulnerability Management, Endpoint Protection, Data Protection, and Reporting and Compliance offerings. Lumension is known for providing world-class customer support and services 24x7, 365 days a year.

Headquartered in Scottsdale, Arizona, Lumension has operations worldwide, including Virginia, Florida, Luxembourg, the United Kingdom, Spain, Australia, India, Hong Kong and Singapore. Lumension: IT Secured. Success Optimized. More information can be found at www.lumension.com.



Global Headquarters

15580 N. Greenway-Hayden Loop, Suite 100
Scottsdale, AZ 85260 USA
phone: +1.888.725.7828
fax: +1.480.970.6323

www.lumension.com

Vulnerability Management | Endpoint Protection | Data Protection | Reporting and Compliance

Additional Research



Video: Cutting the Cost of Compliance without Compromising Security

ROI Case Study - Ogren Group Security Business Analysis of EC Suite

Manage Your Critical Risk

Visit our Resource Center

Protect Your Vital Information

Visit our Resource Center