A Wake Up Call
The Harsh Reality of Audit Fatigue
Security and privacy are among the top concerns of our day. Governments at all levels are responding with compliance requirements designed to protect citizens and defend networks.

What is the business impact of this growing number of security and privacy regulations? How are commercial organizations coping with these requirements? What is the cost to businesses?

Those are just a few of the questions that led to this survey, which we believe to be the first attempt to quantify a growing problem for commercial enterprises: audit fatigue.

In this research study, we learned that IT security and privacy regulations can be very complex and costly, and organizations that fail to meet various directives face substantial consequences.

The study also explored techniques organizations are using to comply with security and privacy regulations. Commonly used tools for managing IT security compliance are inefficient and cumbersome, leaving organizations and the teams who manage compliance activities struggling to see the forest for the trees.

With an ever-growing list of compliance requirements, IT personnel and audit teams are struggling to keep up, resulting in an increase in stress-related illness, high staff turnover, and lost focus. IT professionals report a number of critical functions are often forced to take a back seat to compliance activities.

Audit fatigue is a symptom of the growing IT risk management burden that organizations face today. The very real costs of this burden range from implementation expenses and fines to increased health concerns and high turnover. With so much at risk, organizations would do well to find solutions to ease the compliance burden.
Key findings

On average, organizations currently comply with 13 different IT security compliance and/or privacy regulations, which requires a team of 22 dedicated staff.

Organizations spend over $3.5 million each year on activities relating to IT security compliance and/or privacy regulations. This increases to $4.7 million for those complying with 16+ regulations.

Organizations spend about 58 working days each quarter responding to audit evidence requests.

84% of organizations report the varied and cumbersome processes they use for the many different types of audits they face are time consuming.

Over four in five (81%) security professionals report that they personally dread when their organization is audited.

Those found non-compliant in the last 24 months have received an average of eight fines relating to compliance findings, which has cost the organizations an average of more than $460,000.

Approaching nine in ten (86%) believe that compliance is or will be an issue for them when moving systems, applications, and infrastructures to the cloud.

Nearly all (99%) surveyed security professionals believe that their organization would benefit from or would be interested in an automated solution to manage audits.
The state of IT security compliance and privacy regulations

The management of IT security and privacy compliance isn’t just an item on an organization’s to-do list; it’s becoming a business differentiator for modern companies.

As the number of compliance regulations grows, organizations are finding it hard to keep pace.

On average, respondents’ organizations are currently complying with 13 different IT security compliance and/or privacy regulations and require an average of 22 dedicated staff to manage this process. This increases to 28 people for organizations that must comply with 16 or more regulations.

In addition, when it comes to actually completing an audit, organizations require an average of eight people to get the job done. This increases to 12 people for those organizations that must comply with 16 or more regulations.

On average, organizations currently comply with 13 different IT security compliance and/or privacy regulations, which requires a team of 22 dedicated staff.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>18</td>
<td>18</td>
<td>19</td>
<td>23</td>
<td>28</td>
</tr>
</tbody>
</table>

Average number of dedicated people within organizations that work on IT security compliance and/or privacy regulations [base numbers in chart] split by the number of regulations with which respondents’ organizations are currently complying.
It is clear that organizations are taking compliance seriously; running a team of this magnitude costs both time and money, both of which organizations feel could be better spent elsewhere.

Organizations receive over 17 audit requests each quarter on average. Considering that it takes an average of over three working days to respond to a single audit evidence request, organizations are spending around 58* working days on this activity each quarter, which equates to around 90% of a full-time equivalent.

If organizations could reduce the amount of time spent on audit evidence requests and interviews, there are many different activities they’d like their security and compliance teams to focus on instead, like data analysis (63%), innovation (56%), and researching new threats (50%).

*58 working days is calculated by taking the exact average number of audit requests received each quarter (17.0969387755102) multiplied by the exact average number of working days it takes to respond to a single audit request (3.37458193979933).

If able to reduce the time spent responding to audit evidence requests, respondents’ organizations would prefer to do more...

Activities an organization would engage more in if it were able to reduce the amount of time spent responding to audit evidence requests and interviews [base numbers in legend] split by sector. Not showing all answer options.
What are the underlying challenges and difficulties that are causing organizations to need this level of resource? Security professionals report that the processes involved with managing audits are the most time consuming tasks they face, but other areas come a close second. Whether it be handling the numerous privacy touchpoints that come with managing customer data or keeping up to date with the most recent regulatory changes, it’s clear that the compliance challenges organizations must tackle are daunting.

To keep up with the growing number of regulations, organizations are increasing staff and spending millions on compliance activities.

<table>
<thead>
<tr>
<th>Time consuming compliance tasks</th>
<th>84%</th>
<th>16%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Varied and cumbersome processes for many different types of audits</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Managing the numerous privacy touchpoints that come with maintaining customer data</td>
<td>82%</td>
<td>18%</td>
</tr>
<tr>
<td>Managing numerous reference documents and repositories</td>
<td>80%</td>
<td>20%</td>
</tr>
<tr>
<td>Keeping up to date with the most recent changes to all the regulations it adheres to</td>
<td>75%</td>
<td>24%</td>
</tr>
<tr>
<td>Tracking the overlap between regulations</td>
<td>72%</td>
<td>28%</td>
</tr>
</tbody>
</table>

The most time consuming task security professionals face is managing the varied and cumbersome processes for the many different types of audits they face (84%).

Time consuming compliance tasks, combining those who said: “extremely time consuming” with “somewhat time consuming” and “not that time consuming” with “not time consuming at all” [300 respondents].
For many organizations, the time spent on compliance activities is a result of the variety of tools they are using. The majority of organizations still use departmental databases (71%) and soft copies of documents saved on a company server or network (61%) to manage audit evidence requests.

On paper, these tools should facilitate the process as intended, but in reality, they could actually be slowing the organization down and impacting how they handle audit evidence requests. Nearly six in ten respondents (59%) report that the way in which their organization collates evidence is time consuming, and nearly half (46%) are struggling to organize the evidence in a way that is easy to find.
While the tools being used have a part to play, over four in five (84%) security professionals report that teams who handle IT security compliance and privacy regulations in their organization are facing more fundamental challenges. Over half (55%) struggle with the need to hire more staff to cover an increasing workload while over two in five (42%) are handling increased staff turnover. Couple this with over a third (36%) experiencing increased employee sickness due to stress-related illness, and it’s no wonder that staff burnout (33%) and dissatisfaction among employees (22%) are other challenges they face.

Furthermore, the thought of an impending audit and gathering inaccurate evidence is enough to send shivers down the spine of security professionals. Over three quarters (77%) agree that they worry their organization will face fines if the audit evidence they collect isn’t accurate, and over four in five (81%) personally dread when their organization is audited.

On average, organizations that have been found non-compliant have received eight fines relating to compliance findings.

This increases to 11 for those that have to comply with 16 or more regulations.

On average, organizations that have faced fines paid more than $460,000 over the last 24 months.

Those that have to comply with 16 or more regulations have paid over $600,000 in fines in that time period.

Over four in five (81%) security professionals report that they personally dread when their organization is audited.

While organizations battle with time consuming processes and tools that are perhaps more of a hindrance, there are also secondary effects that could have major consequences. While they have the best intentions to be found in compliance with each audit, they aren’t always successful. On average, respondents’ organizations have been found non-compliant six times in the past 24 months, both by internal and external auditors.

Being found non-compliant has many consequences for organizations, especially now that a glowing compliance record gives a company a competitive advantage. However, arguably the most substantial consequences are the fines and other costs associated with failure to comply. If you combine this figure with the amount of money organizations have spent on compliance activities in the first place, it’s astounding just how much investment organizations have put toward remaining compliant.
A focus on cloud compliance

Given its ability to boost efficiency and increase flexibility, it is no wonder that cloud computing is becoming increasingly popular within respondents’ organizations.

In the next 12 months, they expect to host only 27% of their systems, applications, and infrastructures in an on-premises environment. Around a quarter will reside in public (26%) and private clouds (28%), while nearly two in ten (19%) expect to use hybrid cloud environments.

While operating in the cloud has obvious benefits for organizations, it also comes with its own compliance challenges. Approaching nine in ten (86%) believe that compliance is or will be an issue for them when moving systems, applications, and infrastructures to the cloud. This issue only intensifies as organizations deal with an increasing number of regulations, highlighting just how much of a hurdle cloud compliance is perceived to be.

Respondents who believe that compliance is/would be an issue when moving systems, applications, and infrastructures to the cloud

<table>
<thead>
<tr>
<th>Number of Regulations</th>
<th>Percentage Who Believe Compliance is an Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-6</td>
<td>74%</td>
</tr>
<tr>
<td>7-9</td>
<td>84%</td>
</tr>
<tr>
<td>10-12</td>
<td>85%</td>
</tr>
<tr>
<td>13-15</td>
<td>92%</td>
</tr>
<tr>
<td>16 or more</td>
<td>92%</td>
</tr>
</tbody>
</table>

Percentage who believe that compliance is an issue or think compliance would be an issue for their organization when moving systems, applications, and infrastructures to the cloud [base numbers in graphic] split by the number of regulations with which respondents’ organizations are currently complying.
The challenges organizations face or expect to face when it comes to IT security compliance and privacy regulations in the cloud center around data. Whether it is keeping track of what data is stored in the cloud, how many instances of that data are stored, or its geographic location, data is a source of concern for organizations, especially when complying with numerous regulations.

These findings make it clear that while the cloud can offer organizations an abundance of benefits, it could also be the cause of many compliance headaches.

**IT security compliance challenges in the cloud**

- Keeping track of what sensitive data is stored in the cloud: 60%
- Keeping track of how many instances of sensitive data exist at any one time: 54%
- Placing trust in the cloud provider to handle data compliantly: 50%
- Maintaining uniformity between different environments: 43%
- Keeping track of which countries sensitive data is stored in: 40%

The challenges organizations face or would face when it comes to IT security compliance and/or privacy regulations in the cloud [300 respondents].
The future is automated auditing solutions

As organizations navigate through the minefield of IT security compliance and privacy regulations, they should feel safe in the knowledge that there is a key to unlocking a more streamlined auditing experience.

The key to streamlining audits is automation, and organizations are interested.

Nearly all (99%) respondents believe that there would be benefits for their organization if they were to use an automated solution to manage IT security audits. It's clear that while organizations are looking to reduce the time they spend on audits, the main goal is to gather more accurate evidence, which in the long run will save them money and ensure they are compliant with the ever-increasing number of regulations.

Three quarters of organizations (75%) are cautious when it comes to thinking about implementing an automated solution; nearly four in ten (39%) are concerned about the cost to implement such a system, and similar proportions (38%) are concerned about how long it would take to implement. But while there might be trepidation, nearly all (99%) security professionals believe their organization would benefit from such a system.

Benefits organizations would gain if they were to use an automated solution to manage audits [300 respondents].

- Increase the accuracy of evidence: 54%
- Reduce time spent being audited: 51%
- Respond to audit requests quicker: 50%
- Track regulation changes more easily: 47%
- Reduce duplicated evidence: 45%
- Create one source of information: 45%
- Holistic view of risk and compliance: 34%
- Fail less audits: 28%
Organizations have responded by dedicating numerous staff and investing millions of dollars in this activity, but current efforts aren’t hitting the mark.

The ways in which organizations are currently responding to IT security and privacy audit evidence requests is cumbersome and riddled with pain points, which practitioners themselves readily admit. This is causing organizations to face fines for non-compliance, further adding to the growing expense of compliance activities.

And IT security professionals foresee new challenges as their organizations embrace cloud computing. The number of regulations organizations are required to meet increases as they move more operations to the cloud, creating additional regulatory obstacles.

These issues are causing security professionals untold stress and putting additional strain on their teams. With the majority personally dreading security and privacy audits and many experiencing stress-related illness and decreasing job satisfaction as a result, combating audit fatigue should be a top priority for organizations.

Simplifying compliance processes promises many benefits – reduced workload for already strained IT security personnel, increasing employee satisfaction and retention; limited reputational damage that comes with failing an audit; and increased savings in expensive compliance activities and costly fines. Organizations are looking for ways to realize these benefits by streamlining compliance activities and automating audit processes.

Conclusion

The importance of privacy and security has grown exponentially over the last five years, bringing with it a host of regulations.

Organizations have responded by dedicating numerous staff and investing millions of dollars in this activity, but current efforts aren’t hitting the mark.

The ways in which organizations are currently responding to IT security and privacy audit evidence requests is cumbersome and riddled with pain points, which practitioners themselves readily admit. This is causing organizations to face fines for non-compliance, further adding to the growing expense of compliance activities.
Methodology:
Telos Corporation commissioned independent market research agency Vanson Bourne to conduct the 2020 audit fatigue research. Conducted during July and August 2020, the study surveyed 300 IT security professionals from U.S. organizations with 1,000 or more employees across the private sector, including financial services, IT technology and telecoms, energy, and others.

All interviews were conducted using a rigorous multi-level screening process to ensure that only suitable candidates were allowed to participate.

About Telos Corporation:
Telos Corporation empowers and protects the world's most security-conscious organizations with solutions for continuous security assurance of individuals, systems, and information. Telos' offerings include cybersecurity solutions for IT risk management and information security; cloud security solutions to protect cloud-based assets and enable continuous compliance with industry and government security standards; and enterprise security solutions to ensure that personnel can work and collaborate securely and productively. The company serves military, intelligence and civilian agencies of the federal government, allied nations and commercial organizations around the world. The company is a recipient of the prestigious James S. Cogswell Outstanding Industrial Security Achievement Award from the Defense Security Service (DSS), awarded to less than .03% of eligible organizations.

For more information, visit www.telos.com and follow the company on Twitter @TelosNews.

About Vanson Bourne:
Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.

For more information, visit www.vansonbourne.com.